

powered by

MSSP
GLOBAL



citizensec

citizensec

Киберқауіпсіздік журналы

Білім — бұл қорғаныс.
Біз сізге тәуекелдерді түсінуге көмектесеміз және өзіңіз бен жақындарыңызды
қорғауды бірге үйренеміз.

2025



Назар аударыңыз!

CitizenSec киберқауіпсіздік журналы — бұл сізді көгілдір экрандардан, вирустардан және басқа да киберқауіптерден қорғайтын практикалық кеңестер жинағы.

10 жылдық тәжірибесі бар сарапшылардың нақты ұсыныстар жиынтығы.



Бір рет үйреніп алыңыз, үнемі деңіз және ардайым өзіңізді қорғаңыз!

citizenssec - кибергигиена және әдістеме

powered by mssp.global

"CitizenSec" — mssp.global сарапшылары мен ҚР ЦДИАӨМ Ақпараттық қауіпсіздік комитетінің мамандары бірлесіп жасаған жоба.

Материал киберқауіпсіздік саласындағы 10 жылдан астам тәжірибеге негізделген.

Біздің МИССИЯМЫЗ

— цифрлық әлем үшін қажетті білім мен дағдыларды үйрету арқылы кибермәдениетті арттыру.

Мазмұны

Әлеуметтік инженерия. Алаяқтар қалай әрекет етеді? 06

Алаяқтардың адамдарды жаңылдыру үшін қолданатын әдістері мен психологиялық тәсілдерін анықтап, оларды тануды үйреніңіз.

Фишинг және спам 09

Фишингтік алаяқтықтың негізгі әдістері және қауіпсіздікке арналған тәжірибелік ұсыныстар.

Сенімді құпиясөз қандай болуы керек? 15

Сенімді құпиясөздерді қалай жасау керектігін және қандай құпия сөздерді бұзу оңай екендігін біліңіз.

Don't touch my phone! 18

Сіздің телефоныңыз жеке деректерден қаржылық ақпаратқа дейін барлығын сақтайды. Оны қауіптерден қалай қорғауға болатынын біліңіз.

Шын ба? Wi-Fi бар ма? 21/23

Фактчекинг, жалған хабардан қалай қорғануға болатынын және Wi-Fi-ды қауіпсіз пайдаланудың барлық жолдарын үйреніңіз.

Алыңыз - қол қойыңыз 25

Жеке деректеріңіз бен активтеріңізді қауіпсіздікте сақтау үшін біздің кеңестерімізді қолданыңыз.

Ақшаны көрсет! 30

Қаржылық қауіпсіздік: ақшаны алаяқтардан қалай қорғауға болады?

Балалар - біздің болашағымыз 32

Балаларыңызды интернеттегі киберқатерлерден және алаяқтардан қорғаудың қарапайым тәсілдері.

Талаптарды орындамасаңыз, сіздің шотыңыз бұғатталады.

02

Әлеуметтік инженерия. Алаяқтар қалай әрекет етеді?

Алаяқтар адамдарды жаңылдыру үшін қандай әдістер мен психологиялық тәсілдерді қолданады және оларды тануды қалай үйренуге болады.

Сіздің тіркеулік жазбаңыз 24 сағат ішінде бұғатталады.

Біз сіздің тіркеулік жазбаңызда күдікті әрекеттерді анықтадық. Жеке тұлғаңызды растау үшін сілтеме бойынша өтіп, деректеріңізді растаңыз. Егер сіз бұл әрекетті орындамасаңыз,

Әлеуметтік инженерия

Әлеуметтік инженерия — бұл құпия ақпаратты алу, зиянды бағдарламаны белсендіру немесе алаяққа қажетті әрекеттерді орындау үшін жасалатын манипуляция.

- Алаяқтар сіздің эмоцияларыңызбен манипуляция жасап сізді ойланбастан әрекет етуге мәжбүрлейтін қорқыныш немесе қуаныш сезімін тудырады, шұғылдық және сенімділікті пайдаланады. Оған қарсы тұру үшін, алаяқтардың әдістерін түсіну маңызды:

Алаяқтардың
әдістері



Қорқыныш пен шұғылдықты пайдаланады.



7h ago

Егер сіз талаптарды орындамасаңыз,
сіздің шотыңыз бұғатталады.

Мен сіздің банкіңізден
хабарласып тұрмын,
сізге қатысты жеке
ақпаратты растауымыз
қажет.

**Беделді ұйымдардың
өкілдері болып
көрінеді.**

Сіздің шотыңызда күдікті
операция тіркелді.
Транзакцияны болдырмау
үшін 10 минут ішінде карта
деректерін растаңыз.

**Шұғылдық арқылы
қысым көрсетеді.**

Сіз біздің ең үздік
клиенттеріміздің
бірісіз, біз сізге
арнайы ұсыныс
жасағымыз келеді.

**Жылы сөздер арқылы
сенімділікті арттырады.**

Мыңдаған адамдар
бұл ұсынысты
қолданып үлгерді.

**Барлығы солай
істейді деп
сендіреді.**



Егер хабарлама сіздің **эмоцияларыңызды** қозғап
жатса, кідіріс жасаңыз. Ойланбастан жеке
деректеріңізді бермеңіз, асығыс ақша аудармаңыз.

Ақпаратты ресми арналар арқылы тексеріңіз немесе
ұйымға тікелей қоңырау шалыңыз.

03

Фишинг және спам.

Фишингтік алаяқтықтың негізгі әдістері
және өзіңізді қорғау жолдары.

Фишинг

— бұл балық аулау сияқты, бірақ мақсаты — сіздің деректеріңізді ұрлау.

Фишингтік шабуылдар электрондық пошта, СМС немесе мессенджерлер арқылы жасанды хабарламалар жіберіп, сезімтал деректерді енгізуге итермелеу жолымен көрініс табады.

Фишинг

Классикалық әдіс, жалған хаттар мен сілтемелер арқылы құпия деректерге қол жеткізу.

SEO-фишинг

Шынайы болып көрінетін және іздеу нәтижелерінің жоғарғы жағында пайда болатын жалған сайттар.

Вишинг

Алаяқтар телефон арқылы қоңырау шалып, ақпарат алу үшін түрлі сценарийлер ойлап табады.

Смишинг

СМС немесе мәтіндік хабарламалар арқылы жалған ақпарат жіберу әдісі.

Малвертайзинг

Онлайн жарнамаға кіріктірілген зиянды бағдарлама.

Spear-фишинг

Белгілі бір адамға қатысты жиналған деректерге негізделген мақсатты фишинг.

Спам-фишинг

Фишингтік хаттардың жаппай таралуы.

Фишингті қалай тануға болады?

1 Шешім қабылдауға асықпаңыз, біраз кідіріп ойланыңыз.

2 Назар аудару керек белгілер:

- Хаттағы немесе жіберушінің мекенжайындағы қателер.
- Жіберушінің пошта мекенжайы мен кіріктірілген сілтемелерін тексеріңіз.
- Эмоцияларға әсер ететін ақпаратты сақтықпен қабылдаңыз.
- Сайттың мекенжай жолын тексеріңіз.

3 Күдікті қосымшаларды ашпаңыз.

4 Жорамалдамаңыз, әрқашан тексеріңіз.

5 Алдау мен тиімді ұсыныстарға алданбаңыз, салқынқандылықты сақтаңыз.

Фишинг анатомиясы

Фишингтік шабуылға сенімді контент жасау:

1. Көбінесе өзекті тақырыптар пайдаланылады.
2. Жалған сайттарға сілтемелер немесе зиянды қосымшалары бар жалған электрондық хаттар дайындалады.

001

002

003

Құрбандардың назарын аудару және алдау:

Шұғыл немесе эмоциялық тұрғыдан әсер ететін хабарламалар пайдаланылады (мысалы, «Акцияның аяқталуына бірнеше сағат қалды»).

Фишинг хаттарын жаппай тарату:

Жаппай таратуға арналған серверлерді немесе хаттардың заңды көрінуі үшін бұзылған тіркеулік жазбалары арқылы жіберіледі.

Деректерді және құпия ақпараттарды алу:

Хаттағы сілтеме заңды көрінетін
жалған сайтқа жібереді.

004

005

Ұрланған деректерді пайдалану:

Құрбандардың шынайы
тіркеулік жазбаларына
кіру үшін алынған
деректер қолданылады.

006

Іздерді жасыру:

Ұсталмау үшін жалған
сайттарды, хаттарды
жіберуге пайдаланылған
аккаунттар жойылады.

007

Бұл енді агент...

**Құпиясөздерді
қалай табады
және олардың бұл
әрекеті неге сәтті
болады?**

04

Сенімді құпиясөз қандай болуы керек?

Сенімді құпиясөздерді қалай жасау керектігін
және қандай құпия сөздерді бұзу оңай екендігін
біліңіз.

80%

Статистика:

бұзылған тіркеулік жазбалардың
80%-ы кең таралған
құпиясөздерді қолданған.

Тіпті Марк Цукерберг барлық тіркеулік жазбаларында бірдей құпиясөз қолданғаны үшін бұзылған.

Таныс жағдай ма?

Біз сенің де кейде солай жасайтыныңды білеміз. Әрине, барлық құпиясөздерді есте сақтау қиын...

Сонымен қатар, кибер әлемде брутфорс деген ұғым бар. Бұл алгоритмнің көмегімен барлық мүмкін комбинацияларды таңдау арқылы құпия сөздерді табу әдісі. Әлсіз, қарапайым құпиясөздер бірнеше секунд ішінде бұзылуы мүмкін.



Шешім: Құпиясөз менеджерін қолданыңыз.

Парольдердің маңыздылығы бойынша түрлері:

Қарапайым маңыздылық:

Бұл құпиясөздер күнделікті тапсырмалар мен қолжетімсіз болған жағдайда үлкен қауіп тудырмайтын сервистер үшін қолданылады.

- Әлеуметтік желілер.
- Электрондық пошта сервистері.
- Мессенджерлер.
- Түрлі сайттар мен онлайн-дүкендер.

Жоғары маңыздылық:

Бұл құпиясөздер құпия және сезімтал деректерге қолжетімділікті қорғайды.

- Банктік тіркеулік жазбалар мен қаржылық қосымшалар.
- Қатқыл дискін шифрлау.
- Құпиясөздер менеджеріне қолжетімділік.
- Әкімшілік қолжетімділігі бар тіркеулік жазбалар.

Кеңес:

Құпиясөздер менеджері барлық құпиясөздерді қауіпсіз сақтауға және әрбір тіркеулік жазба үшін бірегей, күрделі комбинацияларды қолдануға көмектеседі. Бұл бұзылу қаупін азайтып, деректеріңізді қорғайды.

Барлық құпиясөздерді бір жерде **сақтамаңыз**.

Оларды маңыздылығына қарай бөліңіз (жоғарыда көрсетілгендей).

Құпиясөздер менеджерін қолданыңыз. Олар құпиясөздерді қауіпсіз сақтауды және басқаруды қамтамасыз етеді.

Күрделі және бірегей құпиясөздерді жасаңыз. Ол үшін құпиясөздер менеджерлеріндегі кіріктірілген генераторларды қолданыңыз.

Егер сіз өз құпиясөзіңізбен бөлісетін болсаңыз, оны бөліктерге **бөліп** жіберіңіз. Толық құпиясөзді бір сервистің көмегімен жібермеңіз. Мысалы, құпиясөздің бір бөлігін мессенджер арқылы, ал қалған бөлігін қоңырау немесе басқа байланыс арнасы арқылы жіберіңіз.

Ұсынылатын менеджерлер: Dashlane, 1Password, KeyPassXC, Bitwarden, Enpass.

05

Do not touch my phone!

Сіздің телефоныңызда — жеке деректерден бастап қаржылық ақпаратқа дейін бәрі сақталады. Оны қауіптерден қалай қорғауға болатынын біліңіз.

Гаджеттерді қорғау

Гаджеттер — бұл бізге қажетті барлық ақпаратымызды сақтауға мүмкіндік беретін қуатты қалта компьютерлері.



Мәселе:

Зиянды қосымшалар сіздің жеке және қаржылық қауіпсіздігіңізге қауіп төндіреді, банктік деректер мен құпиясөздерді ұрлайды. Сонымен қатар заманауи алаяқтық схемаларына биометриялық деректерді жинау үшін жасалатын бейнеқоңыраулар кіреді.

Бұл алаяқтарға сіздің атыңыздан несие рәсімдеуге және қаржылық операциялар жүргізуге мүмкіндік береді.

Шешім:

Біздің құрылғыларымызды қорғаудың негізгі шаралары:

- 1** Құрылғыны қорғау үшін күрделі құпиясөз, ПИН-код орнатыңыз және биометрияны қолданыңыз.
- 2** Электронды құрылғыларыңызға қосымшаларды тек ресми көздерден жүктеңіз: Google Play немесе App Store қосымшаларының қауіпсіздік дейгейі жоғарырақ болып табылады.
- 3** Сенімді антивирус зиянды бағдарламаларды анықтап, бұғаттауға көмектеседі.
- 4** Қосымшалардың сіздің деректеріңізге қолжетімділігін шектеңіз.
- 5** Құрылғының қолданыстағы орнын бақылауға және ұрланған жағдайда деректерді қашықтан өшіруге мүмкіндік беретін функцияларды қосып қойыңыз.
- 6** Құрылғы ұрланған немесе бұзылған жағдайда маңызды деректерді жоғалтпау үшін олардың көшірмесін үнемі жасап жүріңіз.

06

Шын ба?

Фактчекинг және дезинформация:
қалай қорғануға болады?



Фактчекинг және дезинформация: қалай қорғануға болады

Дезинформация — бұл адамдарды әдейі шатастыруға бағытталған жалған ақпарат. Ал мисинформация — бұл жалған немесе қате ақпаратты абайсызда тарату. Екеуі де сенімсіздікке, қоғамдағы поляризацияға және зиянға әкеледі.

Фейктерді таратпау үшін:

- Жаңалықтарды ресми дереккөздер мен Factcheck.kz, StopFake.kz сияқты фактчекинг платформаларынан тексеріңіз.
- Сын тұрғысынан ойлау мен медиасауаттылықты дамытыңыз, бұл сізге объективті деректерді бейтарап пікірлерден ажыратуға көмектеседі.
- Жеке деректерді қорғауға мұқият болыңыз. Интернетте немесе әлеуметтік желілерде жариялаған кез келген ақпаратыңызды алаяқтар өз мүдделеріне пайдалана алатынын ұмытпаңыз.

07

Wi-Fi бар ма?

Wi-Fi-ды қауіпсіз пайдалану
жолдары.

Қоғамдық Wi-Fi желілерін демалыс кезінде немесе саяхаттарда қолдану өте ыңғайлы, бірақ олар қауіпсіз болмауы мүмкін. Қоғамдық қауіптер мен өзіңізді қорғау тәсілдерін қарастырайық.

Қоғамдық Wi-Fi желілерінің мәселелері мен қауіптері:

Шифрлаудың болмауы:

Көптеген желілер деректерді шифрламайды, бұл жеке ақпаратты (құпиясөздер, қаржылық деректер) ұрлауға мүмкіндік береді.

"Ортадағы адам" шабуылы:

Алаяқтар сіз бен желі арасында берілетін деректерді ұстап алуы мүмкін. Нәтижесінде: Сіздің деректеріңіз өзгертіліп немесе ұрлануы мүмкін.

Жалған кіру нүктелері:

Алаяқтар шынайы көрінетін жалған желілерді жасайды, қосылған жағдайда сіздің деректеріңізге қол жеткізе алады.

Wi-Fi-ды қауіпсіз пайдалана отырып саяхаттау жолдары:

- 1 VPN қосыңыз:** Қоғамдық желіге қосылған кезде әрқашан VPN қосыңыз. VPN сіздің деректеріңізді шифрлайды және оларды ұстап алудан қорғайды.
- 2 Желіні тексеріңіз:** Желінің шынайылығына көз жеткізіңіз, мекеме қызметкерлерінен сұраңыз. Күдікті атаулары бар желілерден аулақ болыңыз.
- 3 Автоматты қосылуды өшіріңіз:** Құрылғыңыздың параметрлерінде ашық желілерге автоматты түрде қосылуды өшіріңіз.
- 4 Қаржылық операциялар тек мобильді интернет арқылы:** Қоғамдық желілер арқылы банктік операциялар немесе сатып алулар жасамаңыз.
- 5 Жаңартулар өзектілігі:** Барлық құрылғыларыңыздың қауіпсіздік жаңартуларының өзектілігін тексеріңіз.
- 6 Екі факторлы аутентификация:** Барлық маңызды аккаунттар үшін екі факторлы аутентификацияны қосыңыз.

8cmfp1c

08

Алыңыз – қол қойыңыз!

Жеке деректеріңіз бен активтеріңізді қалай қорғауға
болатынын біздің кеңестерімізден біліңіз.

item count:

total:

card: ****5677987

auth: 586843379

cardholder:



Жеке не дербес деректер

- бұл белгілі бір азаматқа қатысты немесе сол деректер арқылы анықталатын ақпарат.

1. Жалпыға қолжетімді **дербес деректер**: Сіздің келісіміңізбен басқа адамдарға қолжетімді болуы мүмкін ақпарат (мысалы, аты-жөніңіз, ЖСН, мекенжайыңыз).
2. **Шектеулі қолжетімді деректер**: Күпиялылықты сақтауды талап етеді, және заңмен қорғалатын күпияларды қамтиды (мысалы, медициналық, қаржылық немесе коммерциялық деректер).

Идентификациялық деректер: ЖСН, аты-жөні, туған күні, төлқұжат деректері.

Байланыс деректері: Тұратын мекенжайы, телефон нөмірі, электрондық пошта.

Қаржылық деректер: Банктік шот нөмірі, кірістер мен шығыстар туралы ақпарат.

Медициналық деректер: Медициналық жүгіну тарихы, талдау нәтижелері.

Білім туралы деректер: Білім деңгейі, сертификаттар, дипломдар.

Кәсіби деректер: Жұмыс орны, лауазымы, кәсіби дағдылары.

Отбасы жағдайы туралы деректер: Некеге қатысты ақпарат, балалар, басқа туыстар.

Қозғалыс туралы ақпарат: Барған орындарының тарихы, геолокация.

Назар аударыңыз!

Деректеріңізді қолдануға рұқсат бермес бұрын, келесі жайттарға назар аударыңыз:



- **Деректерді жинау және өңдеу мақсаттары:** Олар не үшін жиналады?
- **Деректерді сақтау мерзімі:** Деректеріңіз қанша уақыт пайдаланылатын болады?
- **Үшінші тұлғаларға деректерді беру мүмкіндігі:** Олар кімге және не үшін берілуі мүмкін?
- **Шекарааралық беру:** Деректеріңіз шетелге берілуі мүмкін бе?
- **Деректердің жариялылығы:** Деректеріңіз жариялана ма?

Сіздің құқықтарыңыз заңмен қорғалған

Қазақстанда дербес деректерді қорғау бірнеше заңдармен реттеледі:

- ҚР "Дербес деректер және оларды қорғау туралы" заңы: Деректерді жинау және өңдеуді, сондай-ақ азаматтардың құқықтарын реттейді.
- ҚР "Ақпараттандыру туралы" заңы: Ақпараттық жүйелердегі деректерді қорғайды.
- Азаматтық кодекс: Жеке және отбасылық құпияны қорғау құқығына кепілдік береді.
- Қылмыстық кодекс және Әкімшілік құқық бұзушылық туралы кодекс: дербес деректер туралы заңнаманы бұзғаны үшін жауапкершілікті белгілейді.

Сіздің құқықтарыңыз

Деректеріңізді кім және қалай
өңдеп жатқандығы туралы
ақпарат алу.

Өз деректеріңізді өзгерту немесе
жою.

Оларды өңдеуге берген
келісіміңізді қайтарып алу.

Құқықтарыңыз бұзылған жағдайда не істеу керек?

Егер деректеріңіз заңсыз жиналса немесе пайдаланылса:

- 1** Бұзушылыққа жол берген ұйымға жүгініп, дербес деректеріңізді жоюды талап етіңіз.
- 2** ҚР ЦДИАӨМ Ақпараттық қауіпсіздік комитетіне e-otinish порталы арқылы шағым жіберіңіз.
- 3** Шағымда көрсету керек ақпараттар:
 - Аты-жөніңіз және байланыс деректеріңіз.
 - Бұзушылықтың толық сипаттамасы.
 - Дәлелдер (скриншоттар, хаттар, ұйымның атауы және т.б.).

Деректеріңізді қалай қорғауға болады?

- Деректерді өңдеуге келісім бермес бұрын құпиялылық саясатының шарттарын мұқият оқыңыз.
- Әлеуметтік желілерде сезімтал ақпаратты жарияламаңыз.
- Күрделі құпиясөздерді қолданыңыз және оларды үшінші тұлғаларға бермеңіз.
- Деректеріңізге кімнің қолжетімділігі бар екенін үнемі тексеріп отырыңыз.

ЭЦҚ қауіпсіздігінің құпиялары

Электрондық цифрлық қолтаңба (ЭЦҚ) – бұл электронды құжаттарға қол қоюға және олардың түпнұсқалығын растауға арналған құрал. Ол сіздің жеке деректеріңізді және құжаттарыңызды қорғау үшін пайдаланылады. ЭЦҚ қағаздағы қолтаңбаның электронды баламасы болып табылады.

Қауіптер:

Егер алаяқтар сіздің ЭЦҚ жеке кілтіңізге қол жеткізсе, олар сіздің атыңыздан құжаттарға қол қоя алады.

Қорғаныс шаралары:

- + Кілттерді қорғалған жерде сақтаңыз (смарт-карталар, USB-токендер).
- + ЭЦҚ-мен жұмыс істеуге арналған бағдарламалық жасақтаманы жаңартып отырыңыз.
- + Күрделі құпиясөздерді пайдаланыңыз және оларды үнемі өзгертіп отырыңыз.
- + **Пайдаланылмайтын немесе жоғалған электрондық цифрлық қолтаңба кілттерін қайтарып алыңыз!** Бұл өте маңызды, себебі алаяқтар көбінесе осы кілттерге қол жеткізуге талпынады.

Жауапкершілік:

ЭЦҚ-ны қорғау шараларын қабылдамағаны үшін, сондай-ақ ЭЦҚ-ны үшінші тұлғаларға бергені үшін әкімшілік құқық бұзушылық туралы кодекстің 640-бабының 4 және 5-тармақтарына сәйкес әкімшілік жауапкершілік қарастырылған.

Сонымен қатар, Қылмыстық кодекстің 205-бабына сәйкес, ақпараттық жүйеге заңсыз қол жеткізгені үшін қылмыстық жауапкершілік көзделген.

09

Ақшаны көрсет!

Қаржылық қауіпсіздік: ақшаны алаяқтардан қалай қорғауға болады?



Мәселелер

- **Фишинг:** Деректерді ұрлау үшін жасалған жалған сайттар/хаттар.
- **Скимминг:** Банкоматтарға құрылғылар орнатып, банк карталарының деректерін көшіру.
- **Несиелік алаяқтық:** Сіздің атыңызға заңсыз несие рәсімдеу.

Шешімдер

- +** **Банкоматтарды тексеріңіз:** Банкоматтарда скиммерлердің (пернетақтадағы немесе карта енгізу орнында күдікті элементтердің) бар-жоғын тексеріңіз.
- +** **"Стоп-кредит" функциясын қосыңыз:** Сіздің келісіміңізсіз несие рәсімдеуді болдырмау үшін "Стоп-кредит" функциясын egov.kz сайты немесе мобильді қосымша арқылы қосыңыз .
- +** **Қауіпсіз онлайн-төлемдер:** Тек тексерілген сайттар арқылы сатып алуларды жасаңыз. Онлайн төлемдер үшін жеке карта пайдаланыңыз: Картадағы қаражатты төлем соммасына сәйкестендіріңіз .
- +** **3D Secure:** Операцияларды растау үшін SMS-кодтарды алу мақсатында банк арқылы қорғанысты қосыңыз.
- +** **Екі факторлы аутентификация (2FA):** Банктік қосымшалар мен сайттарда қосымша қорғанысты орнатыңыз.

10

Балалар – біздің болашағымыз

Балаларыңызды интернеттегі киберқатерлер
мен алаяқтардан қорғаудың қарапайым тәсілдері.

Балаларға арналған киберқауіпсіздік

Жасанды интеллект және технологиялар туралы оқиға:

Жақында алаяқтар жасанды интеллектті пайдаланып, баланың ата-анасының атынан жалған дауыстық хабарлама жасаған жағдай болды. Балаға белгісіз адаммен мектептен шығып кету туралы өтінішпен қоңырау шалынды, бұл қоңырауды жіберген "анасы" деп айтылды. Алайда баланың қырағылығы мен дұрыс үйретілгендігі арқасында ол жағдайдың күдікті екенін түсініп, ересектерге хабарлады. Бұл оны ауыр зардаптардан құтқарды.

Контентті шектеу:



Кеңес: DNS және роутер баптауларын қолданып, қажетсіз сайттарға қолжетімділікті шектеңіз.

Мысал: OpenDNS, Яндекс DNS-сервері немесе Google SafeSearch сияқты DNS қызметтерін орнатып, контентті сүзгіден өткізіңіз.

Ата-ана бақылауы:



Кеңес: Баланың интернеттегі белсенділігін қадағалау үшін Google Family Link сияқты ата-ана бақылауы қосымшаларын орнатыңыз.

Жасанды интеллект технологияларын пайдалану:



Кеңес: Дауысты немесе бетті жасанды интеллект арқылы өзгерту сияқты заманауи технологиялар туралы хабардар болыңыз. Балаларыңызға интернеттегі барлық нәрсе шындыққа сай келмейтінін түсіндіріңіз.

Оқиға: Балаларға алаяқтардың жалған видео немесе дауыстық хабарламалар жасау арқылы қалай алдайтыны туралы оқиғаларды айтып беріңіз.

Балаңызбен арнайы код сөзі:

code

Кеңес: Балаңызбен бірге арнайы код сөз ойлап табыңыз. Бұл сөз балаға төтенше жағдайларда мәселені сізге қауіпсіз және байқалмай жеткізуге мүмкіндік береді.

1

Үздіксіз диалог:

Кеңес: Балаларыңызбен олардың онлайн-әрекеттерін үнемі талқылап отырыңыз және мүмкін болатын қауіптерді түсіндіріңіз.

2

Қауіпсіздікті үйрету:

Кеңес: Балаларыңызды күдікті хабарламалар немесе ұсыныстар сияқты қауіпті жағдайларды анықтауға үйретіңіз.

3

Байланыстарды тексеру:

Кеңес: Балаларыңыздың интернетте кіммен сөйлесіп жатқанын мұқият тексеріңіз. Оларға интернеттегі барлық адамдар өздерін шынайы таныстырып отырмауы мүмкін екенін түсіндіріңіз.

4

Қауіпсіз орта құру:

Кеңес: Үйде интернетке байланысты көз келген сұрақтар немесе мәселелерді талқылауға болатын қауіпсіз кеңістік жасаңыз. Балаларыңыз кез келген жағдайда сізден көмек сұрай алатынын білсін.

citizensec – кибергигиена және әдістеме

citizen zero sec

powered by

MSSP
GLOBAL



AI & DIGITAL
MINISTRY

citizensec