AI & DIGITAL MINISTRY

ҚАЗАҚСТАНДАҒЫ КИБЕРМӘДЕНИЕТ

AI & DIGITAL MINISTRY

КИБЕРҚАУІПСІЗДІК САЛАСЫНДАҒЫ ЗАҢНАМАЛЫҚ ӨЗГЕРІСТЕР

- Еңбек кодексіне жұмыс берушілер мен жұмысшылардың киберқауіпсіздік және кибермәдениет талаптарын сақтау міндеті енгізілді
- ҚО, ЖАО және КВО-ның кибермәдениет бойынша жыл сайын оқыту өткізу міндеттері белгіленді
- Цифрлық жүйелердің (КВО) киберқауіпсіздігіне жыл сайын аудит жүргізу міндеттелді (хабарламамен)
- ҚО-ның КВО-ға қатысты мемлекеттік бақылау функциясы ҰҚК-ге берілді

НЕГІЗГІ ӘСЕР



Кибертәуекелдерді жүйелі басқаруға көшу



Жауапкершілік



Мемлекеттік бақылау



Жыл сайынғы аудит

ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУҒА ҚАТЫСТЫ ЗАҢНАМАЛЫҚ ӨЗГЕРІСТЕР

AI & DIGITAL MINISTRY

- Шектеулі қолжетімділігі бар жеке деректерге қол жеткізуде қосымша қорғаныс элементі ретінде міндетті биометриялық сәйкестендіру енгізілді
- Жеке деректердің ағып кетуі туралы азаматтарды хабардар ету міндеті бекітілді
- Жеке деректердің ірі операторлары тізілімі енгізіліп, мемлекеттік органдарға өңдеудің басталуы туралы хабарлама жолдау міндеттелді
- Жеке деректер идентификаторларының анықтамасы енгізілді

НЕГІЗГІ ӘСЕР



Жеке деректердің ашықтығын арттыру және олардың қорғалуын қамтамасыз ету

Биометрия

Азаматтарды хабардар ету

Операторлар тізілімі

EGOV СЕРВИСТЕРІ

AI & DIGITAL MINISTRY

eGov mobile-да барлық 4 сервис қолжетімді

СТОП-КРЕДИТ

12,5 млн

азамат eGov-тағы функцияны 2024–2026 жылдар аралығында пайдаланды

NOMADGUARD.KZ

10 мың.

сілтеме фишинг пен зиянды БҚ-ға тексерілді

> 650 мың.

азамат өз деректерін жеке деректердің таралуына тексерді

CITIZENSEC.KZ

81 мың.

пайдаланушы «Халыққа арналған кибергигиена» курсынан өтті

5 мың.

мемлекеттік қызметші «Мемлекеттік қызметшілерге арналған кибергигиена» курсынан өтті

ДҚБ СЕРВИСІ

100%

мемлекеттік цифрлық жүйелер қосылған

463

мемлекеттік және жеке цифрлық жүйе қосылған



КИБЕРМӘДЕНИЕТ АЙЫ

AI & DIGITAL MINISTRY

Мақсаты

Халықтың хабардарлық деңгейін арттыру, киберкеңістікте жауапты әрі қауіпсіз мінез-құлық дағдыларын қалыптастыру, цифрлық гигиенаны дамыту және киберқауіптердің алдын алу.

АУДИТОРИЯ

- барлық жастағы азаматтар
- балалар мен жастар
- бизнес және мемлекеттік органдар
- кәсіби қауымдастық

1. Ақпараттық науқан және медиақолдау
2. Киберсабақтар
3. Өңірлік форумдар, семинарлар және воркшоптар
4. Интернет-алаяқтықтың алдын алу және дербес деректерді қорғау
5. Тестілеу, цифрлық сервистер және кәсіби іс-шаралар
6. Кибермәдениет пен цифрлық қауіпсіздік туралы үздік роликке арналған конкурс

НЕГІЗГІ ІС-ШАРАЛАР

AI & DIGITAL MINISTRY

CYBER CLASS

Іс-шара:
Елдің бірыңғай «Cyber Class» киберсабағы мектептер мен колледждерге арналған

Ұйымдастырушылар:
ОАМ, ЖИ және ЦДМ, облыстардың, Астана, Алматы және Шымкент қалаларының әкімдіктері, білім беру ұйымдары

Күні:
2026 жылғы қыркүйек

Өтетін орны:
Қазақстан Республикасының бүкіл аумағындағы мектептер мен колледждер

CYBER STEPPE

Іс-шара:
Кибермәдениет стандарт ретінде: қауіпсіздік моделін қайта құру

Ұйымдастырушылар:
ЖИ және ЦДМ, облыстардың, Астана, Алматы және Шымкент қалаларының әкімдіктері, білім беру ұйымдары

Күні:
2026 жылғы 10–11 қыркүйек

Өтетін орны:
Астана, Мәңгілік Ел даңғылы, 55/1, B1 блогы

KAZ HACK STAN

KazHackStan-2026

Іс-шара:
Киберқауіпсіздік жөніндегі халықаралық конференция

Ұйымдастырушылар:
ЖИ және ЦДМ, TSARKA

Күні:
2026 жылғы 29–30 қыркүйек

Өтетін орны:
Тәуелсіздік сарайы, Астана қ.

FORTINET

Fortinet Security Day

Іс-шара:
Практикалық сессиялары бар сарапшылық конференция

Ұйымдастырушылар:
Fortinet және серіктес ұйымдар

Күні:
2026 жылғы 15 қыркүйек

Өтетін орны:
Ritz-Carlton, Астана қ.

АЙМАҚТЫҚ ФОРУМДАР

AI & DIGITAL MINISTRY



АУТЕНТИФИКАЦИЯ КЕЗІНДЕГІ ҚАУІПСІЗДІК

AI & DIGITAL MINISTRY

ТІРКЕЛГІ ЖАЗБАЛАРДЫ ҚОРҒАУДЫҢ 7 ЕРЕЖЕСІ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІ

Қазақстан Республисасының Жасанды интелілект және цифрлық даму министрлігі

БҰЛ НЕ ҮШІН МАҢЫЗДЫ

31% құпиясөз ретінде баласының атын немесе туған күнін пайдаланады

44% жеке және жұмыс тіркелгілері үшін бір ғана құпиясөзді пайдаланады

14% жұмыс құпиясөздерін серіктесімен бөліскен

11% жұмыс құпиясөздерін отбасы мүшелерімен бөліскен

34% өз командасының ішінде құпиясөздермен алмасқан

01

Күрделі құпиясөз қолданыңыз

12 таңбадан артық. Әріптер, сандар және белгілердің кездейсоқ комбинацияларын қолданыңыз.

LastPass: құпиясөз генераторы
https://www.lastpass.com/features/password-generator

Security.org: құпиясөзді бұзу уақытының бағасы
https://www.security.org/how-secure-is-my-password/

02

Құпиясөзді қайталамаңыз және ешкімге бермеңіз

Әр сервис үшін бөлек құпиясөз қолданыңыз.
Оны ешкімге айтпаңыз.

03

Құпиясөз менеджерін пайдаланыңыз

Bitwarden: құпиясөздерді сақтау https://bitwarden.com

KeePass: офлайн сақтау https://keepass.info

04

Екі факторлы аутентификацияны қосыңыз

Кіруді қосымша фактормен растаңыз.

05

Резервтік кодтарды сақтаңыз

Қалпына келтіру кодтарын қауіпсіз жерде сақтаңыз.

06

Деректердің жылыстауы туралы хабарламаларға жазылыңыз

Firefox Monitor: деректердің жылыстауын тегін бақылау.
Тіркелгіңізідің таралған дерекқорларда бар-жоғын тексеріңіз.
https://monitor.firefox.com

07

Бөгде құрылғыдан абайлап кіріңіз

Chrome браузерінде инкогнито режимін қолданыңыз: Ctrl+Shift+N / Cmd+Shift+N.
Жұмысты аяқтаған соң аккаунттан шығып, терезені жабыңыз.

2021 жылғы статистика: Keeper Security — 31%; TechRepublic — қалған көрсткіштер.

Құпиясөздерді тексеру сервисінде тек оқу мысалдарын пайдаланыңыз.

ВЕБ-САЙТТАРДЫ ҚАУІПСІЗ ҚАРАУ ЕРЕЖЕЛЕРІ

AI & DIGITAL MINISTRY

01



Жарнама аз болса — интернетте жылдамырақ, қауіпсіз әрі ыңғайлы!

Жарнаманы бұғаттау

Қажетсіз жарнамаларды бұғаттау үшін uBlock Origin кеңейтімін пайдаланыңыз:

- **Mozilla Firefox** – https://addons.mozilla.org/addon/ublock-origin/
- **Google Chrome** – https://chrome.google.com/webstore/detail/ublock-origin/
- **Microsoft Edge** – https://microsoftedge.microsoft.com/addons/detail/ublock-origin/
- **Opera** – https://addons.opera.com/extensions/details/ublock/

02



Сайттарды тексеріңіз — деректерінізді қорғаңыз!

Веб-сайттың ресми екеніне көз жеткізіңіз

Деректерді енгізер алдында сайттың ресми екеніне көз жеткізіңіз. Мысалы, kaspik.kz — Kaspi Bank-тің ресми емес сайты. Ресми сайт — kaspi.kz.

Егер күмәніңіз болса, сайт мекенжайын VirusTotal арқылы тексеріңіз:
https://www.virustotal.com/gui/url

ДЕРБЕС КОМПЬЮТЕРДІ ҚАУІПСІЗ ПАЙДАЛАНУ ЕРЕЖЕЛЕРІ

AI & DIGITAL MINISTRY

01

Операциялық жүйе мен бағдарламаларды үнемі жаңартып отырыңыз.

Жаңартулар осалдықтарды жояды және құрылғыңызды қорғайды.

02

Құрылғыңызды шифрлаңыз.

- BitLocker (Windows) – https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption
- FileVault (macOS) – https://support.apple.com/en-us/HT204837
- Linux (LUKS) – https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup

03

Маңызды деректердің резервтік көшірмелерін үнемі жасап отырыңыз.

Деректерді Yandex Cloud, Google Drive, Облако Mail.ru сияқты бұлтты сервистерде сақтаңыз.

Yandex Cloud | Google Drive | облако mail.ru

04

Компьютерге USB-құрылғыларын қосқанда абай болыңыз.

Белгісіз флеш-жинақтауыштарды пайдаланбаңыз — олардың құрамында зиянды БҚ болуы мүмкін.

05

Cortana немесе Siri-ді өшіріңіз.

Дауыстық көмекшілер сіздің сұрауларыңыз туралы деректерді жинап, жібере алады.

06

Пираттық қолданбаларды орнатпаңыз.

Олардың құрамында зиянды БҚ болуы және жүйеде осалдықтар тудыруы мүмкін.

07

Антивирустық бағдарламалық қамтамасыз етуді пайдаланыңыз.

- Microsoft Defender – https://support.microsoft.com/en-us/topic/installing-microsoft-defender-ba7d17d7-464b-444d-bb47-99b07278369d
- Bitdefender Antivirus – https://www.bitdefender.com/
- Malwarebytes – https://ru.malwarebytes.com/

Bitdefender | Windows Defender | Malwarebytes

08

Экран үшін қорғаныш антишпиондық үлдірді пайдаланыңыз.

Бұл экрандағы ақпаратты көзбен шолып көруден қорғауға және деректеріңізді сақтауға көмектеседі.

ҰСЫНЫСТАР | РЕКОМЕНДАЦИИ

AI & DIGITAL MINISTRY

АЗАМАТТАРҒА ҰСЫНЫСТАР

- құпиясөздерді, SMS-кодтарды және растау кодтарын ешкімге хабарламаңыз
- құрылғыларды қорғау үшін антивирустарды пайдаланыңыз
- күмәнді қоңырауларды ресми байланыс арналары арқылы қайта тексеріңіз
- күмәнді сілтемелерге өтпеңіз
- күрделі құпиясөздерді және екі факторлы аутентификацияны пайдаланыңыз
- қосымшаларды ресми дереккөздерден орнатыңыз және жаңартып отырыңыз
- дербес деректерді қорғаңыз және құпия ақпаратты жарияламаңыз

РЕКОМЕНДАЦИИ ГРАЖДАНАМ

- не сообщайте пароли, SMS-коды и коды подтверждения
- используйте антивирусы для защиты устройств
- перепроверяйте подозрительные звонки через официальные каналы связи
- не переходите по подозрительным ссылкам
- используйте сложные пароли и двухфакторную аутентификацию
- устанавливайте и обновляйте приложения из официальных источников
- защищайте персональные данные и не публикуйте конфиденциальную информацию

ГОСУДАРЫҚ ҚЫЗМЕТШІЛЕРГЕ АРНАЛҒАН КИБЕРҚАУІПСІЗДІК БОЙЫНША ҰСЫНЫМДАР

AI & DIGITAL MINISTRY

- мемлекеттік органдардың (МО), жергілікті атқарушы органдардың (ЖАО) қызметшілері өздерінің қызметтік міндеттерін орындау кезінде электрондық нысандағы қызметтік хат алмасуда тек ведомстволық электрондық поштаны пайдаланады
- Интернет желісіне қосылу тек Интернетке қол жеткізудің бірыңғай шлюзі арқылы жүзеге асырылуы қажет
- Интернет желісінің ресурстарымен және электрондық поштамен жұмыс істеу кезінде қызметкерге қызметтік қажеттілікке байланысты немесе өзге жолмен белгілі болған мемлекеттік, қызметтік және коммерциялық ақпаратты жариялауға тыйым салынады

- мемлекеттік органның (МО) ішкі желілерін Интернетке қосуға тыйым салынады
- компьютерлер мен Интернет желісін қараусыз ашық күйде қалдыруға тыйым салынады. Жұмыс орнынан кеткен жағдайда компьютерді міндетті түрде бұғаттау қажет (Windows+L пернелер тіркесімі)
- мемлекеттік органның бірыңғай көліктік ортасына (ЕТС), жергілікті желісіне сымсыз желілер, сымсыз қол жеткізу, модемдер, радиомодемдер, ұялы байланыс операторлары желілерінің модемдері және басқа да сымсыз құрылғылар арқылы қосылуға тыйым салынады