SOUTH KAZAKHYSTAN
MEDICAL ACADEMY

КОРПОРАТИВТІК
СЕКТОРҒА
АРНАЛҒАН

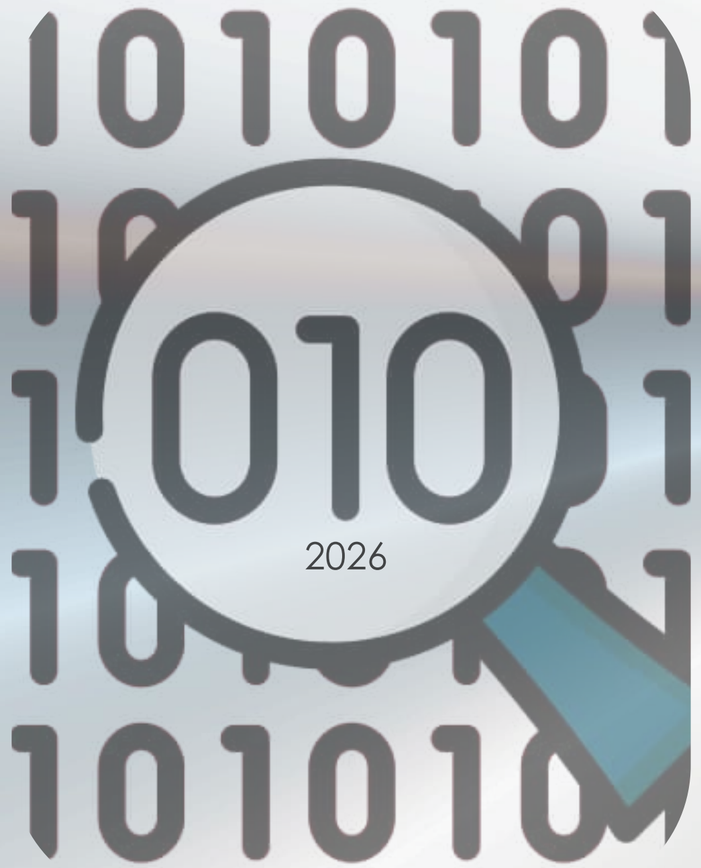
CYBER HYGIENE

2026

Presented By:
SABYRZHAN ARYNBAYEV
CYBERSECURITY AND INFORMATION SYSTEMS PROTECTION SPECIALIST

Корпоративтік секторға арналған

Кибергигиена мазмұны – қысқаша бағдарлама



1-модуль. Ақпараттық қауіпсіздік негіздері
2-модуль. Кибергигиена
3-модуль. Корпоративтік ортадағы кибергигиенаның негізгі ұғымдары
4-модуль. КиберШабуылдар. ФИШИНГ және СПАМ, Әлеуметтік инженерия
5-модуль. Дербес деректер қауіпсіздігі
6-модуль. Қауіпсіз интернет
7-модуль. Құпиясөз саясаты
8-модуль. Цифрлық активтер
9-модуль. Қаржы қауіпсіздігі
10-модуль. AI (Жасанды интеллект) қауіпсіздігі
11-модуль. Мобильді құрылғылар қауіпсіздігі
12-модуль. Өзін өзі дамыту курстарына ұсыныс
13-модуль. Қорытынды

SOUTH KAZAKHSTAN MEDICAL ACADEMY

Ақпараттық қауіпсіздік негіздері

Ақпараттық қауіпсіздік негіздері — бұл ақпаратты рұқсатсыз қолжетімділіктен, ұрланудан, өзгертілуден және жойылудан қорғауға бағытталған шаралар жиынтығы. Ол жеке деректерді сақтау, интернетті қауіпсіз пайдалану, кибергигиена ережелерін сақтау және киберқауіптер мен кибербуллингтің алдын алуды қамтиды.

Киберқауіпсіздік (Cybersecurity)

Киберқауіпсіздік — бұл компьютерлік жүйелерді, желілерді, бағдарламаларды және деректерді кибершабуылдардан, рұқсатсыз қолжетімділіктен, бұзылудан немесе жойылудан қорғауға бағытталған шаралар мен тәсілдер жиынтығы.

Кибербуллинг (Cyberbullying)

Кибербуллинг (Cyberbullying) — интернет, әлеуметтік желілер, мессенджерлер немесе онлайн ойындар арқылы адамды қорлау, мазақ ету, қорқыту, жала жабу немесе психологиялық қысым көрсету.

Кибергигиена (Cyber Hygiene)

Кибергигиена — бұл әрбір қолданушының күнделікті сақтауы тиіс қауіпсіз мінез-құлық ережелері мен әдеттері.

Ол адамның интернет пен цифрлық құрылғыларды қалай қолданатынына тікелей байланысты.

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

КИБЕРГИГИЕНА

2026

Кибергигиена — бұл цифрлық құрылғыларды, желілерді және онлайн-сервистерді қауіпсіз пайдалану үшін арналған ережелер мен тәжірибелер жүйесі. Медициналық жоғары оқу орындары үшін бұл тақырып ерекше маңызды, өйткені болашақ дәрігерлер мен медицина қызметкерлері пациенттердің құпия деректерімен жұмыс істейді және цифрлық медициналық технологияларды қолданады.

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Жалпы медицина қызметкерлері білуі тиіс киберұғымдар:

Кибербуллинг (Cyberbullying)

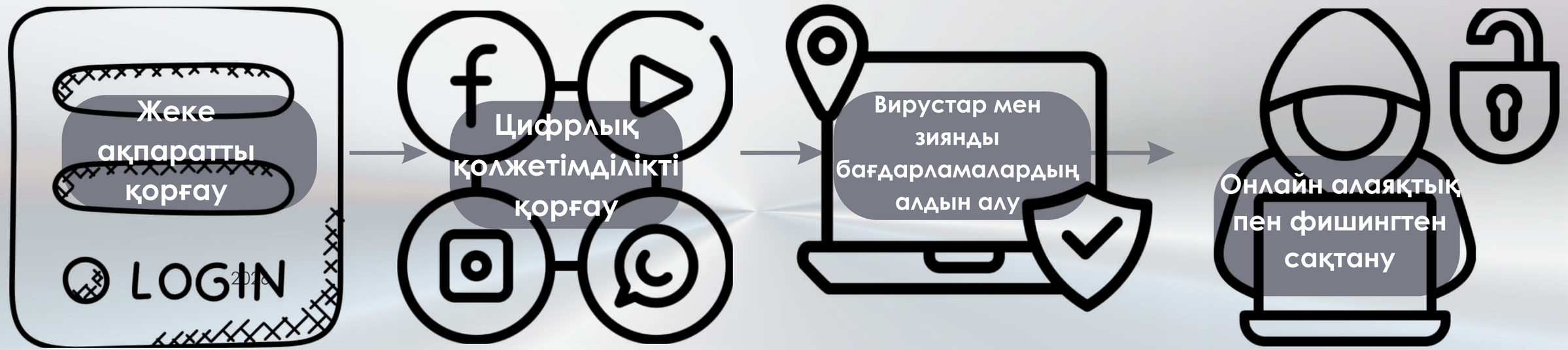
Фишинг (Phishing)

Әлеуметтік инженерия (Social Engineering)

Деректерді ұрлау (Data Breach / Data Leak)

SOUTH KAZAKHSTAN MEDICAL ACADEMY

КОРПОРАТИВТІК ОРТАДАҒЫ КИБЕРГИГИЕНАНЫҢ НЕГІЗГІ ҰҒЫМДАРЫ



Қазіргі цифрлық қоғамда кибергигиена әрбір интернет қолданушысы үшін маңызды. Оқушылар мен студенттерден бастап, мұғалімдерге, мемлекеттік қызметкерлерге және кәсіпкерлерге дейін барлығы киберқауіптерге тап болуы мүмкін. Сондықтан кибергигиенаны сақтау — жеке қауіпсіздіктің ғана емес, сонымен қатар қоғамның жалпы ақпараттық қауіпсіздігінің маңызды бөлігі болып табылады.

SOUTH KAZAKHYSTAN
MEDICAL ACADEMY

Жеке деректер мен активтерді коргау жолдарын біздін кеңестердің көмегімен біліңіз.

CYBER HYGIENE

тауар саны:

барлығы:

карта: ****5677987

аутент: 5868Ч3379

карта иесі:

ЖЕКЕ ДЕРЕКТЕР

SOUTH KAZAKHSTAN MEDICAL ACADEMY

Жалпыға қолжетімді деректер:
Сіздің келісіміңізбен басқа адамдарға қолжетімді болуы мүмкін ақпарат (мысалы: аты-жөні, ЖСН, мекенжайы).

Шектеулі қолжетімді деректер:
Заңмен қорғалатын ақпарат (мысалы: медициналық, қаржылық немесе коммерциялық мәліметтер).

Қаржылық деректер:
Банктік шоттар, табыс пен шығыс туралы ақпарат.

Білім туралы деректер:
Дипломдар, сертификаттар , білім деңгейі.

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

Кәсіби деректер:
Жұмыс орны, лауазымы, кәсіби дағдылары.

Отбасылық жағдай туралы деректер:
Неке, балалар, туыстар туралы ақпарат.

Байланыс деректері:
Тұрғылықты мекенжай, телефон нөмірі, электрондық пошта.

Қозғалыс туралы ақпарат:
Бару тарихы, геолокация деректері.

Жеке деректер — бұл сізді жеке тұлға ретінде анықтайтын кез келген ақпарат.

SOUTH KAZAKHSTAN MEDICAL ACADEMY

НАЗАР АУДАРЫҢЫЗ

Өз деректеріңізді бермес бұрын, мына мәселелерге көңіл бөліңіз:

- **Деректерді жинау және өңдеу мақсаты:** олар не үшін жиналады?
- **Сақтау мерзімі:** деректеріңіз қанша уақыт пайдаланылмақ?
- **Үшінші тұлғаларға беру мүмкіндігі**: кімге және қандай мақсатта берілуі мүмкін?
- **Трансшекаралық бер**у: деректеріңіз шетелге жіберілуі мүмкін бе?
- **Жалпыға қолжетімділігі**: деректеріңіз жариялана ма?

Сіздің құқықтарыңыз заңмен қорғалған Қазақстанда дербес деректерді қорғау бірнеше заңдармен реттеледі:

- ***«Дербес деректер және оларды қорғау туралы» ҚР Заңы*** — деректерді жинау, өңдеу тәртібін және азаматтардың құқықтарын реттейді.
- ***«Ақпараттандыру туралы» ҚР Заңы —*** ақпараттық жүйелердегі деректердің қорғалуын қамтамасыз етеді.
- ***Қазақстан Республикасының Азаматтық кодексі*** — жеке және отбасылық құпияны қорғау құқығын кепілдейді.
- ***Қылмыстық кодекс және Әкімшілік құқық бұзушылық туралы кодекс*** — дербес деректер туралы заңнаманы бұзғаны үшін жауапкершілікті белгілейді.

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Деректер – алтынмен те !

Сіздің құқығыңыз

- **Деректеріңізді кім және қалай өңдейтіні туралы ақпарат алу.**
- **Өз деректеріңізді өзгерту немесе жою.**
- **Деректерді өңдеуге берген келісімді кері қайтарып алу.**

Құқықтарыңыз бұзылған жағдайда не істеу керек?

Егер деректеріңіз заңсыз жиналса немесе пайдаланылса:

Бұзушылық жасаған ұйымға жүгініп, деректерді жоюды талап етіңіз.

ҚР ЦДИАӘМ Ақпараттық қауіпсіздік комитетіне e-Otinish порталы арқылы шағым беріңіз.

Шағымда көрсетіңіз:

- Аты-жөніңіз және байланыс деректеріңіз
- Бұзушылықтың толық сипаттамасы
- Дәлелдер (скриншоттар, хаттар, ұйым атауы және т.б.)

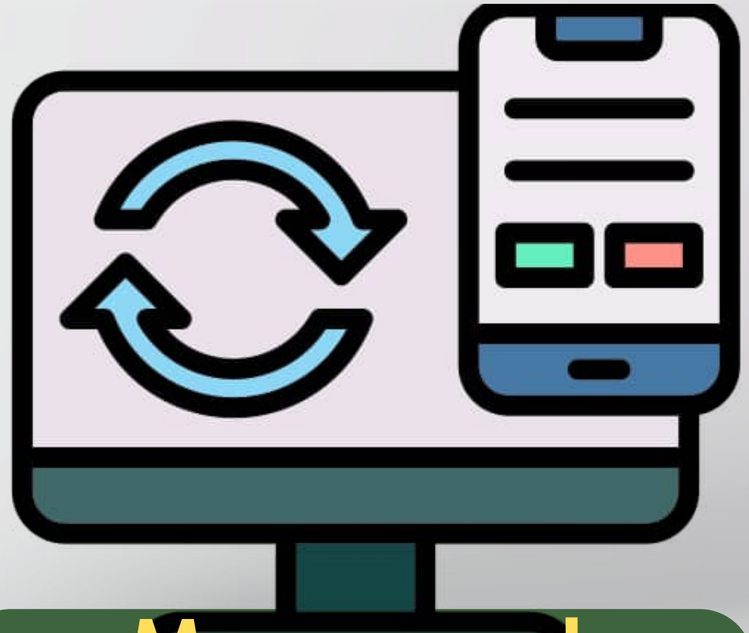
Деректеріңізді қалай қорғауға болады?

Деректеріңізді қалай қорғауға болады?

- Деректерді өңдеуге келісер алдында құпиялылық саясатының шарттарын оқыңыз.
- Әлеуметтік желілерде құпия ақпаратты жарияламаңыз.
- Күрделі құпиясөздер қолданыңыз және оларды үшінші тұлғаларға бермеңіз.
- Деректеріңізге кімнің қолжетімділігі бар екенін үнемі тексеріп отырыңыз.

Кеңес!

⚠ Ақпаратпен абайлап бөлісіңіз: Сезімтал деректерді әлеуметтік желілерде жарияламаңыз және интернетте бөлісетін деректеріңізге қатысты абай болыңыз.

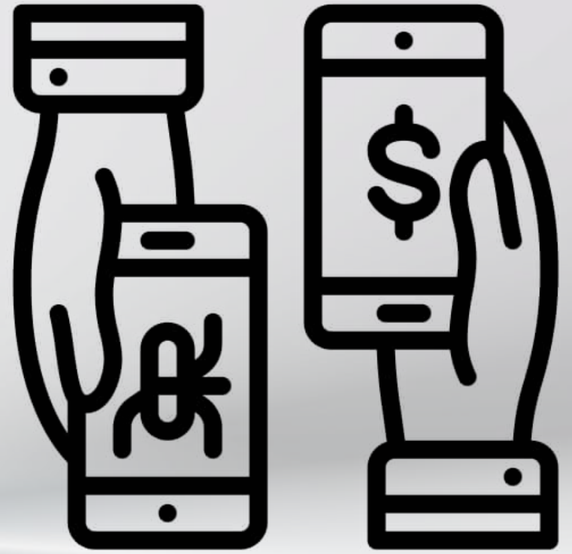


Маңызды!

⚠ Интернетте дербес деректерді қорғау мұқияттылық пен абайлықты талап етеді, бірақ бұл сіздің жеке қауіпсіздігіңіз бен құпиялығыңызды сақтау үшін маңызды!

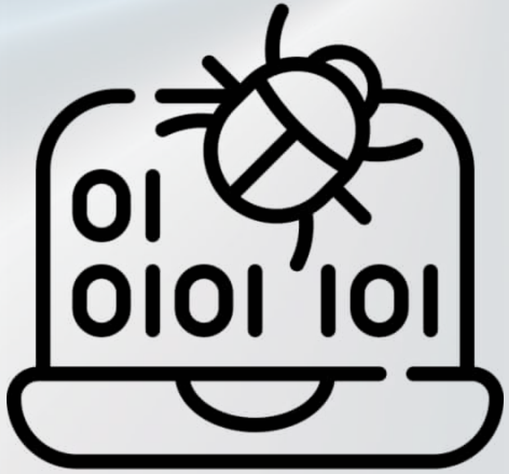
SKMA 1979 SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Қазақстанда жеке деректердің ауқымды таралуы факторлары



Жеке деректердің ауқымды таралуы (2025)
📅 16 маусым 2025 жыл

- Интернетте 16 млн+ азаматтың деректері таралуы мүмкін екені туралы ақпарат шықты
- «Қазақстан тұрғындары 2024» атты архив табылғаны хабарланды
- Мәліметтер ішінде:
  - Аты-жөні
  - ЖСН
  - Телефон нөмірі
  - Тұрғылықты мекенжай
  - Басқа жеке деректер



2025 жылы Қазақстанда 40-тан астам ірі жеке деректердің таралуы тіркелген.

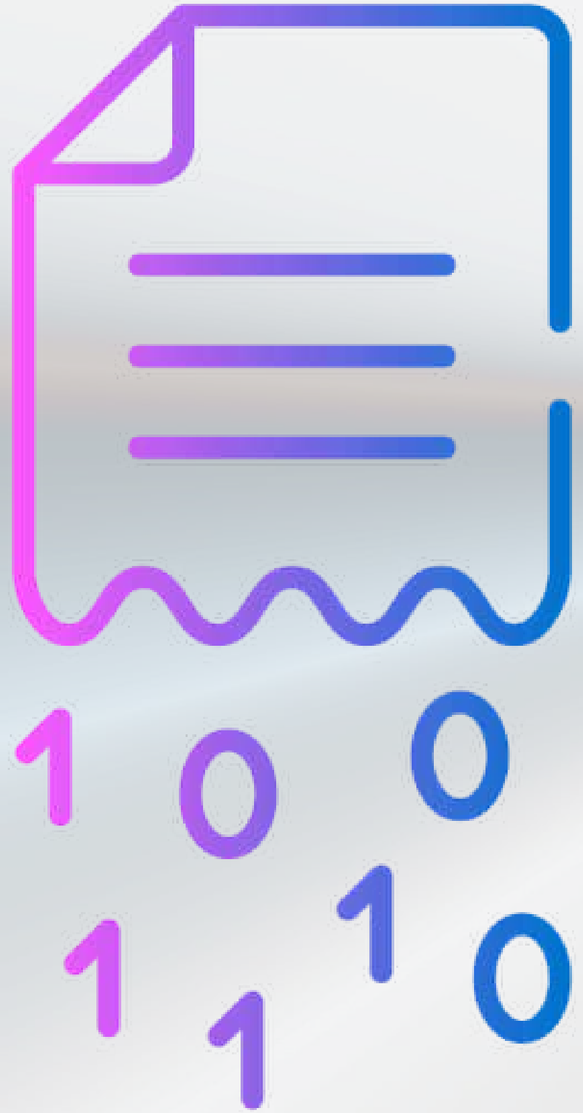
Ең әлсіз буын — жүйе емес, адам.

Яғни, персоналдық деректерге қолжетімділігі бар операторлар мен қызметкерлер.
🔎 Негізгі себеп — адам факторы

Жекеменшік ұйым қызметкерлері персоналдық деректерге заңды қолжетімділігі бар тұлғалар ақылы түрде клиент мәліметтерін үшінші тарапқа сатқан

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Қазақстанда жеке деректердің таралуына 20 млн теңге айыппұл қаупі бар.



Қазақстанда жеке деректердің таралуына жауапкершілікті қатты күшейту жоспарлануда. Жаңа шаралар азаматтардың конституциялық құқығын – жеке өмірге қол сұғылмаушылық пен персоналдық деректерді қорғауды іске асыруға бағытталған.

Қауіпсіздік талаптарын орындамаған ұйымдар мен лауазымды тұлғаларға әкімшілік айыппұл шегі бірнеше есе ұлғайып, ***5 000 МРП (шамамен 21 млн теңге)*** *деңгейіне жетеді.*

- В утечке из Instagram нашли +77 и .kz: что это значит для казахстанцев
- Вице-премьер Мадиев пригрозил госорганам ответственностью за утечку персональных данных
- МинИИ и Kundelik отрицают утечку персональных данных
- Фишинговая атака на Beeline Казахстан: в компании опровергли информацию о взломе и утечке данных
- Была ли утечка: базу интернет-магазинов "Меломан" и "Империя цветов" с заказами и адресами нашли в Сети
- Утечка данных 16 млн казахстанцев: начато расследование

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Цифрлық активтер – бұл заманауи бизнестің негізі. Оларды қорғау әр қызметкердің назарын талап етеді. Ережелерді ұстану және жауапты әрекет ету бағалы ақпаратты және компанияның тұрақтылығын сақтауға көмектеседі.

Компанияның цифрлық активіне қолжетімдігі бар әр қызметкер оның қауіпсіздігі үшін жауапты. Егер сізде қолжетімдік болмауы тиіс нәрсеге қолжетімдік болса, онда бұл туралы қауіпсіздік бөліміне хабарлауға тиіссіз!

1. Жеке деректердің ұрлануы

2. Фишинг және әлеуметтік инженерия

3. Аңду және денеге қауіп төндіру

4. Аккаунттарды бұзу

SOUTH KAZAKHSTAN MEDICAL ACADEMY

Қ ауіп і і і у а

⚠️ **Қауіп**

Егер алаяқтар ЭЦҚ-ның жеке кілтіне қол жеткізсе, олар сіздің атыңыздан құжаттарға қол қоя алады.

🔐 **Қорғану шаралары**

- Кілттерді қауіпсіз жерде сақтаңыз (смарт-карта, USB-токен).
- ЭЦҚ-мен жұмыс істеуге арналған бағдарламаларды үнемі жаңартып отырыңыз.
- Күрделі құпиясөздерді қолданыңыз және оларды тұрақты түрде өзгертіңіз.
- Қолданылмайтын немесе жоғалған ЭЦҚ кілттерін міндетті түрде кері қайтарыңыз (бұғаттаңыз).

❗ Бұл өте маңызды, өйткені көбіне дәл осы кілттерді алаяқтар ұрлайды.

⚖️ **Жауапкершілік**

Әкімшілік жауапкершілік:
— ЭЦҚ-ны қорғау шараларын сақтамағаны және оны үшінші тұлғаға бергені үшін *(ҚР ӘҚБтК 640-бап)*.
Қылмыстық жауапкершілік:
— Ақпараттық жүйеге заңсыз қол жеткізгені үшін *(ҚР ҚК 205-бап)*.

ЭЦҚ-ға қатысты ең жиі инциденттер:

Қазақстандағы ең жиі кездесетін оқиғалар

1. **ЭЦҚ-ны басқа адамға беру ең көп таралған)**

Бұл — ресми түрде тіркелетін ең жиі инцидент.

2. **Бөтен адам ЭЦҚ қолдану фактілері**

2025 жылдан бастап:

- **тек берген адам емес**
- **пайдаланған адам да жауап береді**

Бұл да жиі тіркелетін бұзушылық.

3. **Кілттердің ұрлануы (жеке кілттің компрометациясы)**

Көбінесе:

- **флешка жоғалуы**
- **компьютер вирус жұқтыруы**
- **фишинг**

4. **Ішкі алаяқтық (корпоративтік ортада)**

SOUTH KAZAKHSTAN MEDICAL ACADEMY

SOUTH KAZAKHSTAN MEDICAL ACADEMY
2026

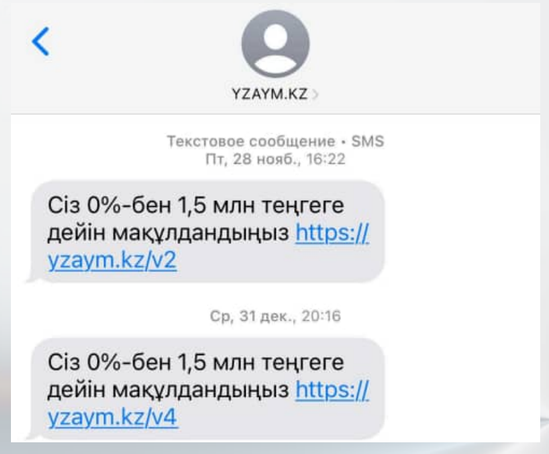
КИБЕРШАБУЫЛДАР

Негізгі шабуыл түрлері: **ФИШИНГ және СПАМ**

Кибершабуылдар *көбіне адам факторы мен жүйедегі осалдықтарды пайдалану арқылы іске асады*

Фишинг

Бұл - балық аулауға ұқсайды, бірақ мақсаты — сіздің деректеріңізді ұрлау. Фишинг шабуылдары электронды пошта, SMS немесе мессенджерлер арқылы жіберілетін жалған хабарламалар арқылы жүзеге асып, пайдаланушыны құпия деректерді енгізуге мәжбүрлейді.

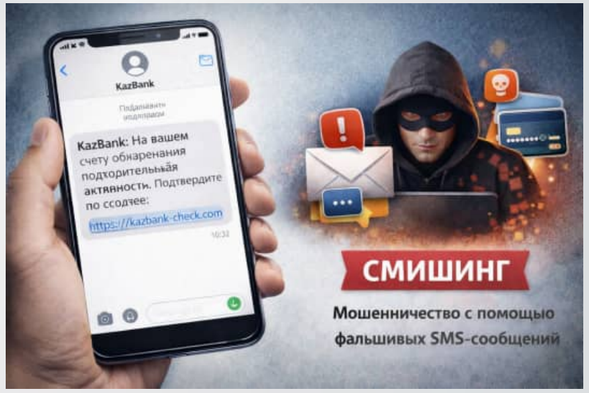


Малвертайзинг

Интернеттегі жарнамаларға зиянды бағдарламаны әдейі енгізу арқылы жасалатын кибершабуыл түрі. Пайдаланушы осындай жарнаманы басқанда, оның құрылғысына вирус жұғуы немесе деректері ұрлануы мүмкін.

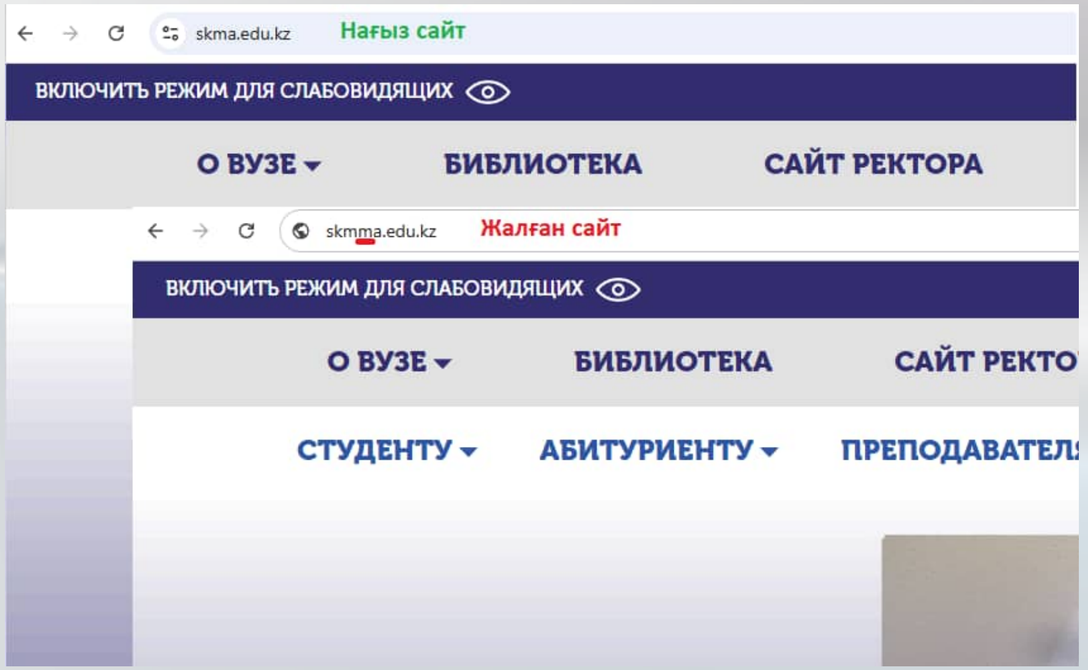
Смишинг

SMS және мәтіндік хабарламалар арқылы жасалатын алаяқтық.



SEO-фишинг

Іздеу жүйелерінде (Google, Yandex т.б.) жоғары орындарға әдейі шығарылған, нағыз сайттарға ұқсас жалған веб-сайттар арқылы пайдаланушыларды алдау әдісі. Мұндай сайттар логин, құпиясөз, банк деректері сияқты ақпаратты ұрлау үшін жасалады.



Спам-фишинг

Фишингтік хаттарды жаппай тарату арқылы жасалатын шабуыл түрі.

Spear-фишинг

Нақты бір адамға бағытталған, ол туралы алдын ала жиналған деректерге негізделген мақсатты фишинг

Вишинг

Алаяқтардың телефон арқылы қоңырау шалып, түрлі сценарийлер ойлап тауып, ақпаратты алдап алу әрекеті.

SOUTH KAZAKHSTAN MEDICAL ACADEMY
2026

КИБЕРШАБУЫЛДАР

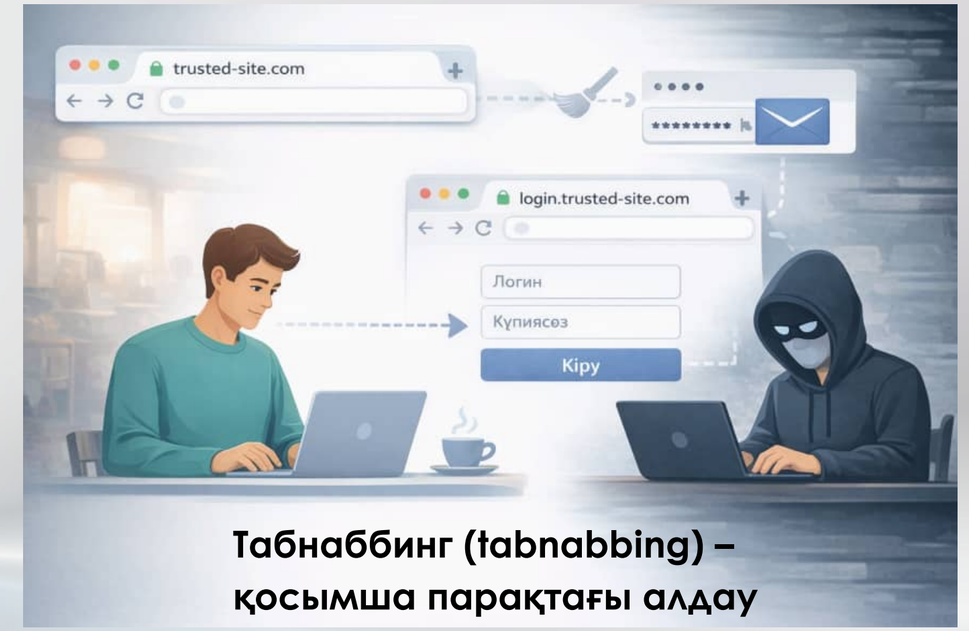
НЕГІЗГІ ШАБУЫЛ ТҮРЛЕРІ: ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ

Тайпсквоттинг (typosquatting) немесе саусақ іздері үшін тұзақ

Қастық ойлаушылар атауында бір-екі әріптік қате бар, танымал сайттарға ұқсас домендерді әдейі тіркейді.

Мысалы, сіз walmart сайтына кіргіңіз келеді, бірақ қателесіп wallmart деп терсеңіз, деректерді ұрлау үшін жасалған жалған сайтқа тап болуыңыз мүмкін.

Бір ғана ұсақ қате — және сіз фишингтік сайтқа кіріп кетесіз.



Табнаббинг (tabnabbing) – қосымша парақтағы алдау

Хакерлер пайдаланушы ашқан, бірақ белсенді әрекет жасалмаған веб-парақты уақыт өте келе жасырын түрде өзгерту әдісін қолданады. Нәтижесінде ол таныс сайтқа ұқсайтын жалған бетке айналады. Пайдаланушы ешқандай күмәнданбай, кейін сол параққа қайта оралып, логин мен құпиясөзін енгізеді. Осы сәтте қаскөйлер бұл деректерді ұстап алып, аккаунтқа рұқсатсыз қол жеткізеді.

«Зұлым егіз» (evil twin).

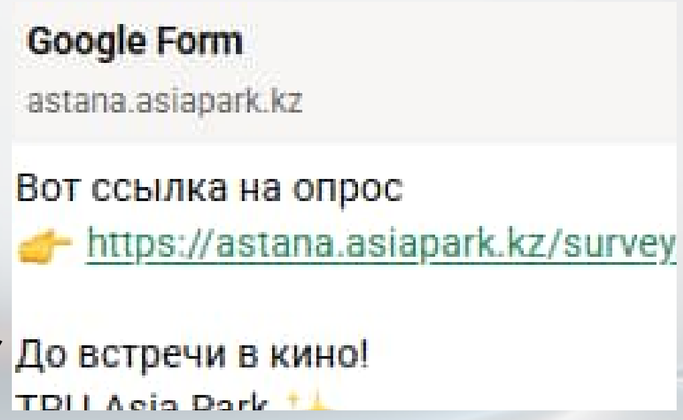
Алаяқтар дәмханаларда, әуежайларда немесе басқа да қоғамдық орындарда нағыз Wi-Fi желісіне ұқсас жалған желі құратын шабуыл түрі. Пайдаланушы сол желіге қосылған кезде, қаскөйлер оның интернеттегі әрекеттерін бақылап, логин, құпиясөз және жеке деректерін ұрлайды

SOUTH KAZAKHSTAN MEDICAL ACADEMY
2026

КИБЕРШАБУЫЛДАР

Кликджекинг

Кликджекинг — пайдаланушыны жасырын сілтемені немесе батырманы басуға алдап мәжбүрлеу арқылы жасалатын шабуыл түрі. Сырттай қауіпсіз болып көрінгенімен, басу нәтижесінде зиянды әрекеттер орын алуы мүмкін, мысалы вирустардың таралуы немесе жеке деректердің ұрлануы.



Бейтинг (Baiting)

Алаяқтар құрбанның құрылғысына қол жеткізу және оны зиянды бағдарламалық жасақтамамен (БЖ) жұқтыру үшін физикалық тасығышты (мысалы, USB-флешканы) әдейі қоғамдық жерде қалдырады. Құрылғыны тапқан адам оны өз компьютеріне қосқан сәтте, жүйеге зиян келтіретін бағдарлама автоматты түрде іске қосылуы мүмкін.

Әлеуметтік инженерия

Бұл адамдарды манипуляциялау әдісі, оның мақсаты – адамды белгілі әрекеттер жасауға немесе құпия ақпаратты ашуға мәжбүрлеу. Қастық ойлаушылар адамның табиғи әлсіздіктерін пайдаланғандықтан, ол жұмыс жасайды:

1. Сенгіштік және көмектесу ниеті
2. Қорқыныш және шешімдер қабылдау жеделдігі
3. Әуестік және мұқиятсыздық

Англер-фишинг (angler phishing).

Алаяқтар өзін шынайы компанияның қолдау көрсету қызметінің қызметкері ретінде таныстырып, пайдаланушыдан ақпаратты алдап алу әдісі. Әдетте бұл шабуыл әлеуметтік желілерде жүзеге асады: пайдаланушы компанияны @ таңбасымен белгілеп жазба қалдырған кезде, алаяқтар сол компания атынан жалған аккаунт арқылы жауап береді. Осылайша олар логин, құпиясөз немесе басқа да жеке деректерді алуға тырысады.

SOUTH KAZAKHSTAN MEDICAL ACADEMY

Фишинг екенін қалай түсінуге болады?

Тоқтаңыз, қараңыз, ойланыңыз!

Ескерту белгілері:

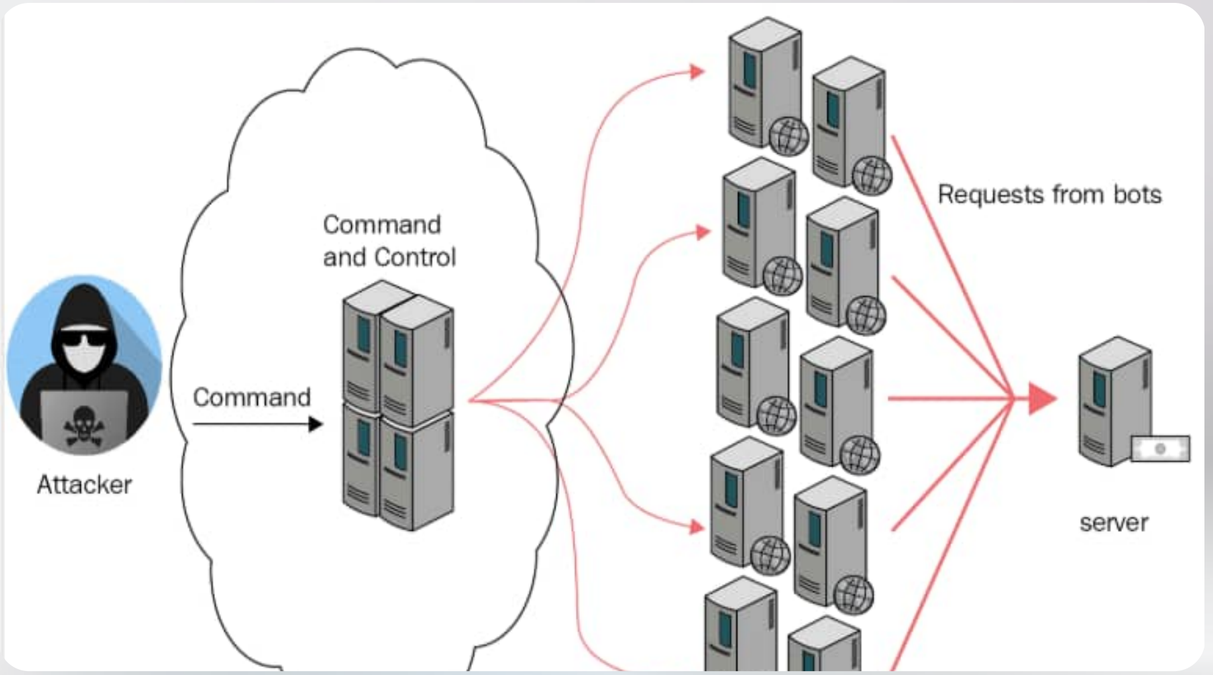
- Хатта немесе мекенжайда қателер болады.
- Жіберушінің адресін және сілтемелерді міндетті түрде тексеріңіз.
- Қатты эмоция тудыратын хаттарға сақ болыңыз (қорқыту, асықтыру, «жедел» талаптар).
- Сайттың мекенжай жолағын (адрес жолын) мұқият тексеріңіз.

Күмәнді тіркемелерді ашпаңыз.

Болжам жасамаңыз, әрқашан тексеріңіз.

Айла-тәсілдерге алданбаңыз және «тым тиімді» ұсыныстарға сенбеңіз, салқынқандылық сақтаңыз.

Желілік шабуыл (network attack)



DDoS шабуыл (Distributed Denial of Service)

DDoS — бұл кибершабуыл түрі, онда шабуылдаушылар серверге немесе желіге өте көп жалған сұраныс жіберіп, оның қалыпты жұмысын тоқтатады.

Шабуыл кезінде:

Хакер мыңдаған жұқтырылған компьютерлерді (ботнет) пайдаланады

Олар бір уақытта мақсатты серверге сұраныс жібереді

Сервердің ресурсы таусылады

Нәтижесінде:

- сайт ашылмайды
- жүйе баяулайды
- қызмет тоқтайды

2026

SOUTH KAZAKHSTAN MEDICAL ACADEMY

Адам факторы бұзудың себебіне айналған кейстер

Медициналық жүйедегі деректердің ұрлануы (утечка данных) (2019)

2019 жылы ірі медициналық ақпаратық жүйелердің бірі арқылы қазақстандықтардың дербес медициналық деректері ұрланды (утечка данных). Деректердің ұрлануының себебі – клиника қызметкерінің абайсыздығы және жеткілікті хабардар болмауы, ол қауіпсіздік ережелерін ұстанбай, деректер базасын тиісті қорғаусыз және ғаламторда ашық күйінде қалдырған. Нәтижесінде мыңдаған пациенттердің медициналық карталары, ЖСН және талдау нәтижелері желіге түсті, бұл күрделі жанжалға әкеп соқты.

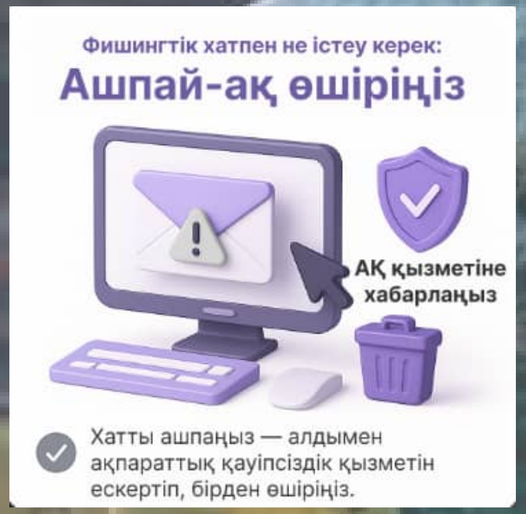
Ірі банкті фишинг арқылы бұзу (2020)

2020 жылы қазақстандық банктердің бірінің клиенттерінің деректерінің жылыстауына байланысты оқыс оқиға орын алды. Оның себебі банк қызметкерлерінің біріне жасалған фишингтік шабуыл болды, ол қызметкер зиян келтіретін сілтемеден өтіп, есептік деректерді енгізіп, қастық ойлаушыларға ішкі банктік жүйелерге қолжетімдік берген. Бірнеше мыңдаған клиенттердің дербес және қаржылық деректері жылыстаған.

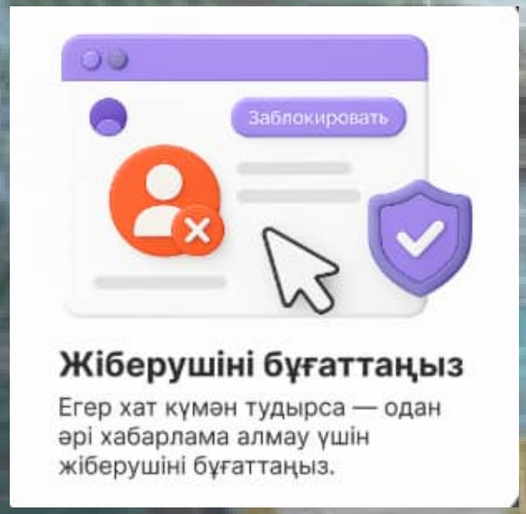
SOUTH KAZAKHSTAN MEDICAL ACADEMY

Кибершабуыл кезінде әрекет ету бойынша ұсыныстар

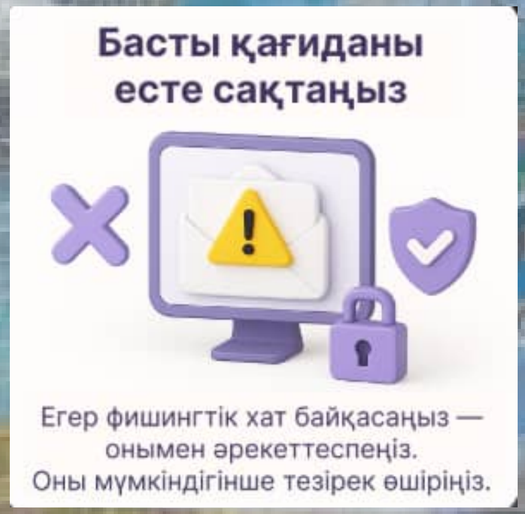
❌ Хатты ашпаңыз, қауіпсіздік қызметіне хабарлап, хатты бірден жойыңыз



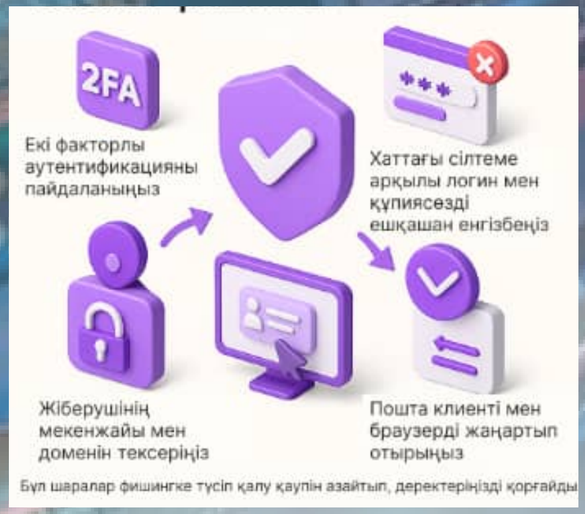
🚫 Жөнелтушіні бұғаттаңыз



🧠 Басты қағиданы есте ұстаңыз



💡 Өзіңізді фишингтен тағы қалай қорғауға болады?



2026

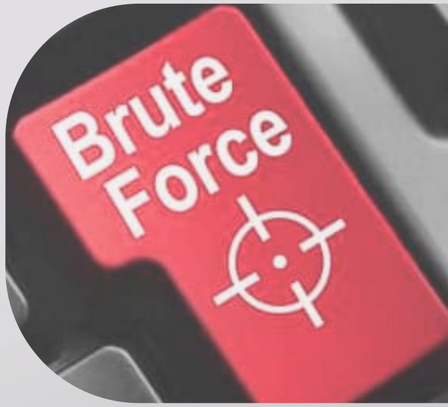
Құпиясөз саясаты

Құпиясөз саясаты ұ

ұ

ұ

ҚҰПИЯ СӨЗ ҚАУІПСІЗДІГІ

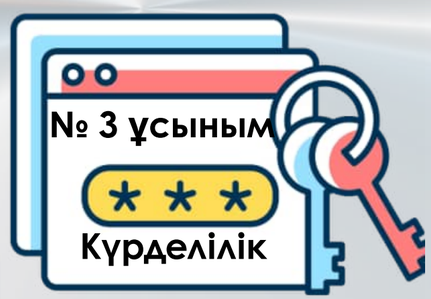


№1 ұсыным

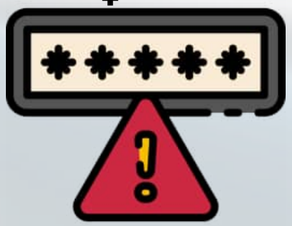
Бірегейлік бірегей құпиясөз қолдану

№ 2 ұсыным

Құпиясөз кем дегенде 14 символдан кем болмауы тиіс (22 символ болғаны тіпті жақсы).



№4 ұсыным



Әріптердің үйлесімі

№5 ұсыным

Цифрлар мен арнайы символдар

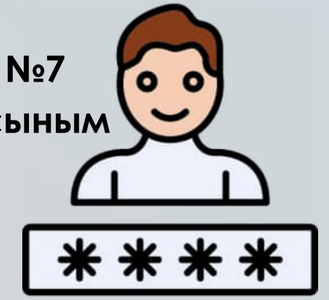
Character class	example	entropy / character (bits)
Only lowercase letters	abc	4.7
+ uppercase letters	aBc	5.7
+ numbers	aBc1	5.95
+ special characters	aB?c1	6.4

Құпиясөздің күш энтропиясы

№6 ұсыным

Сөзсіз пароль

№7 ұсыным



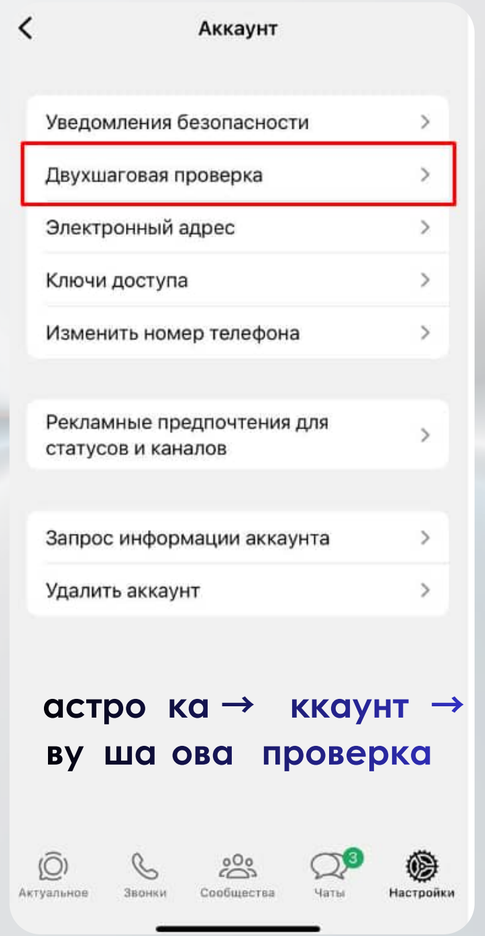
Жеке ақпаратсыз

Екі кезеңді (көп факторлы — 2FA/MFA) аутентификацияны мүмкін болған барлық сервистерде қосып қойыңыз.
Көп факторлы аутентификацияда тек құпиясөзді білу жеткіліксіз: жүйеге кіру үшін қосымша растау да қажет болады. Мысалы, SMS арқылы келген кодты енгізу немесе арнайы қосымшадағы бір реттік кілтті пайдалану керек. Бұл хакерлердің аккаунтқа заңсыз кіруін айтарлықтай қиындатады.

2FA - екі факторлық аутентификация

№9 ұсыным

ұпи сөз менеджерін па даланыңыз



- Әлеуметтік желілер
- Электрондық пошта сервистері
- Мессенджерлер
- Банктік аккаунттар

сынылатын құпи сөз менеджерлері

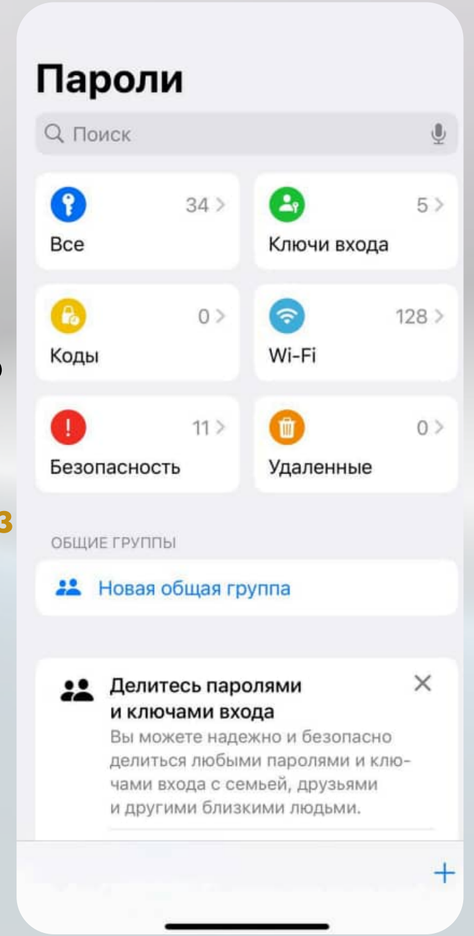
Dashlane

1Password

KeePassXC

Bitwarden

Е ра



SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Құпиясөз қауіпсіздігі статистикасы

Қазақстанда тіркелетін киберинциденттердің шамамен

- **70–80%**-ы әлсіз немесе ұрланған парольдерге байланысты.
- Пайдаланушылардың **60%**-дан астамы
- бір парольді бірнеше сервисте қолданады.
- Қазақстанда тіркелетін кибершабуылдардың ең көп тараған түрі — фишинг және аккаунт бұзу.
- Жыл сайын **20 мыңнан** астам аккаунт заңсыз кіру әрекеттеріне ұшырайды.

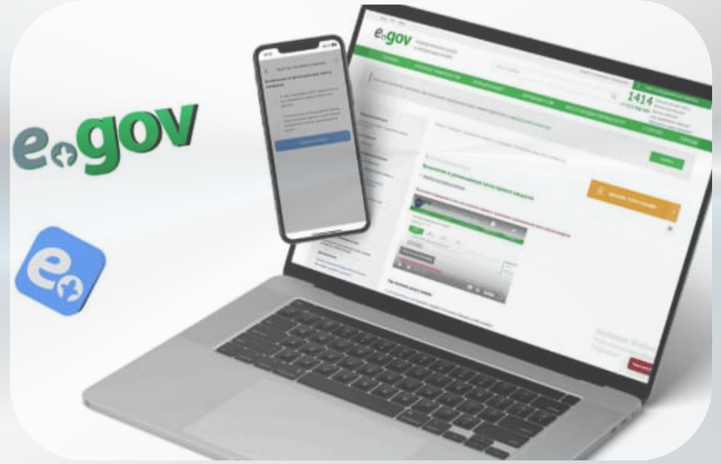
КҰПИЯСӨЗ ҰРЛАНУ ИНЦИДЕНТТЕРІ

Facebook (2016)
Марк Цукерберг аккаунты бұзылды.
Себебі: бірдей құпиясөзді бірнеше сервисте қолданған

LinkedIn деректердің ұрлануы (2012–2021)
100 млн+ аккаунттың логин-парольдері жарияланды
Әлсіз парольдер тез бұзылды

Yahoo! (2013–2014)

- 3 млрд аккаунт деректері ұрланды
- Әлемдегі ең ірі пароль бұзылу оқиғаларының бірі



Мемлекеттік сервистерге фишинг (жыл сайын)

- eGov.kz атынан жалған хаттар таратылады
- Пайдаланушылар парольдерін өздері енгізіп береді

Банктік аккаунттар бұзылуы
Қазақстанда жыл сайын мыңдаған интернет-алаяқтық тіркеледі

SOUTH
KAZAKHYSTAN
MEDICAL ACADEMY

Менің

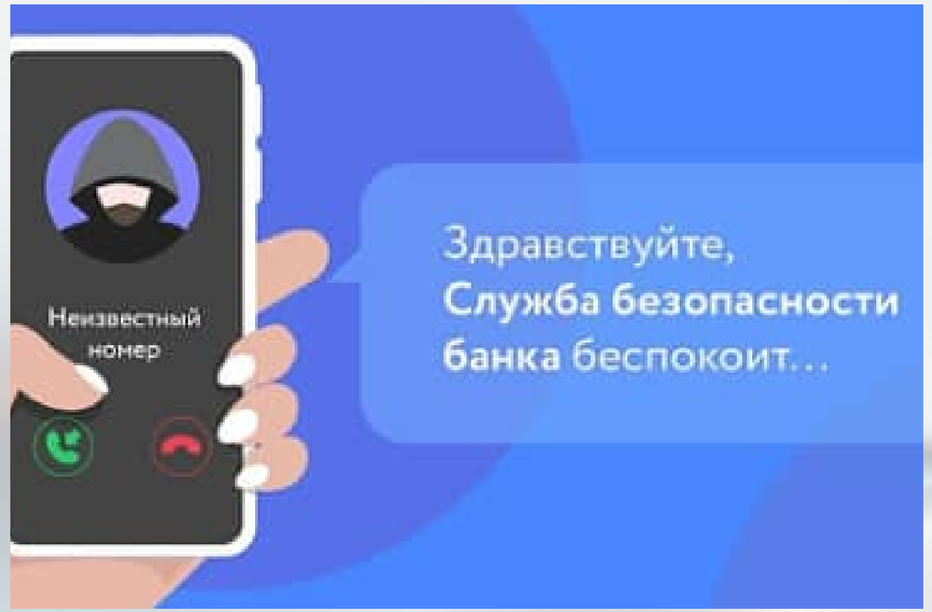
телефонымда

тұрсың!

2026

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Мобильді құрылғылардың қауіпсіздігі



1. **Мессенджерлер мен электрондық пошта арқылы Фишинг**

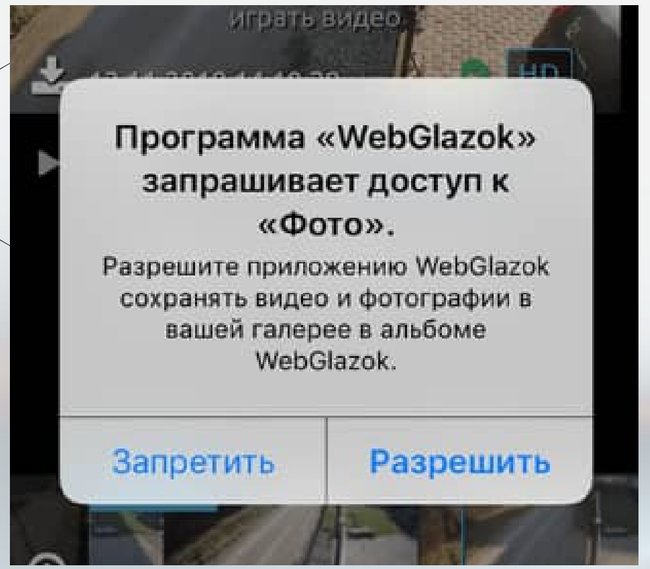
- Жалған сайттарға апаратын алаяқтық сілтемелер.
- WhatsApp, Telegram, SMS арқылы жіберілген және зиян келтіретін коды бар файлдар.

2. Вирус кірген қосымшалар

- Бөгде дүкендердің бағдарламалары (Android-ғы APK-файлдар).
- Тіпті Google Play-де зиян келтіретін кітапханалары бар қосымшалар.

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Мобильді құрылғылардың қауіпсіздігі



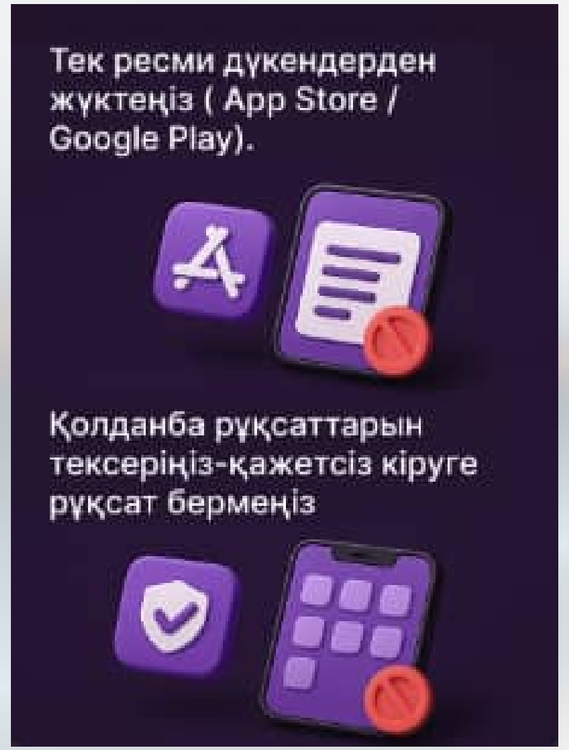
3. Рұқсаттарды теріс пайдалану

Камера, микрофон, геолокация, байланыс нөмірлеріне қолжетімдік пайдаланушының рұқсатынсыз жиі пайдаланылады.

4. SIM-карта (SIM-swap) арқылы шабуылдар жасау

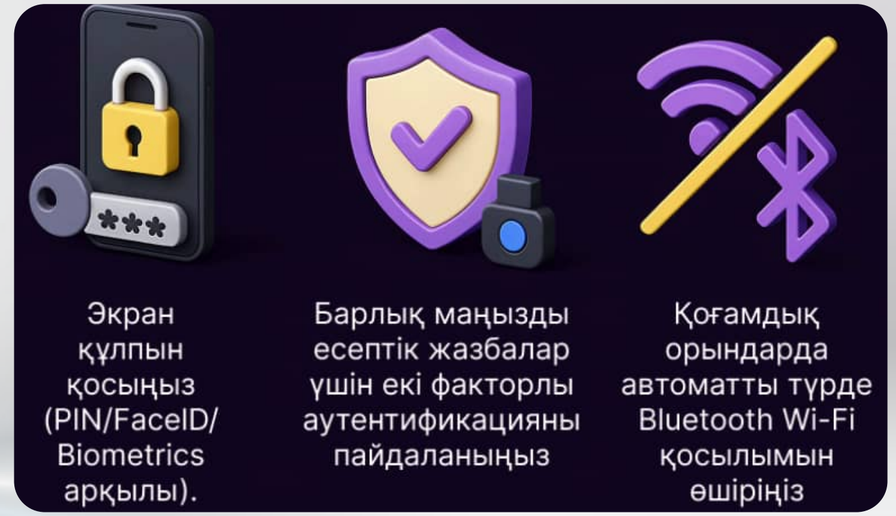
Қастық ойлаушы құрбанның деректерін басқа SIM картаға ауыстырады, SMS пен шалынған қоңыраулары ұстап қалады.

🚨 Смартфонды қорғау бойынша ұсынымдар



🛡️ **Қосымшаларды орнату:**

Ресми дүкендерден ғана жүктеңіз (App Store / Google Play).

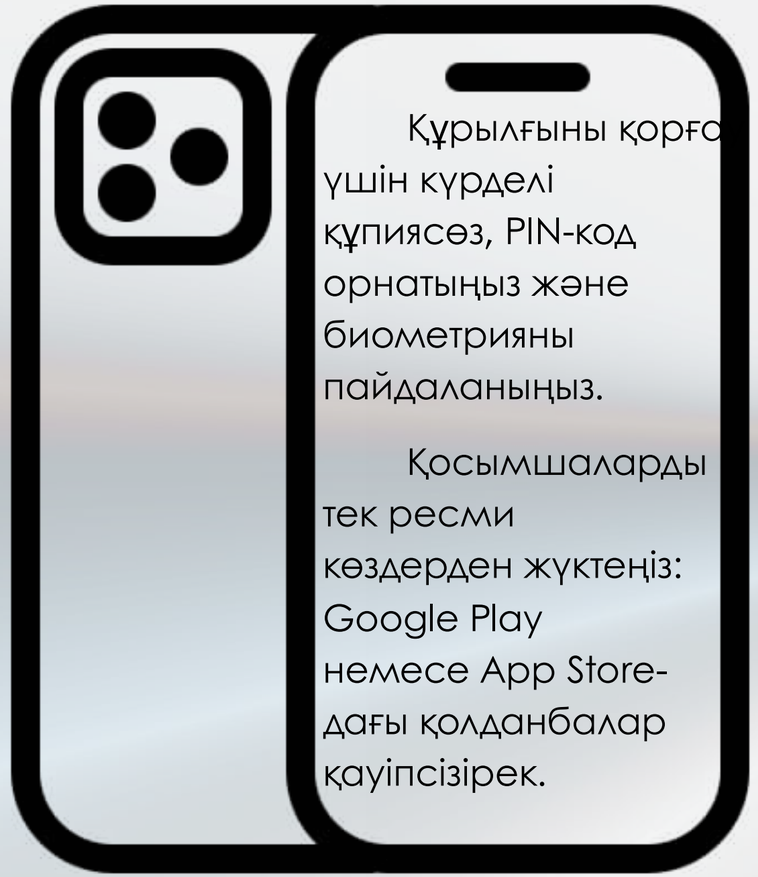


Жаңартулар:

Патчтар шыққан кейін операциялық жүйені және қосымшаны бірден жаңартыңыз.
Егер БЖ жаңартуы шықса, бірақ сізге қолжетімді болмаса, онда бұл құрылғыға шпиондық БЖ кіргізілгенінің айқын белгісі болуы мүмкін.

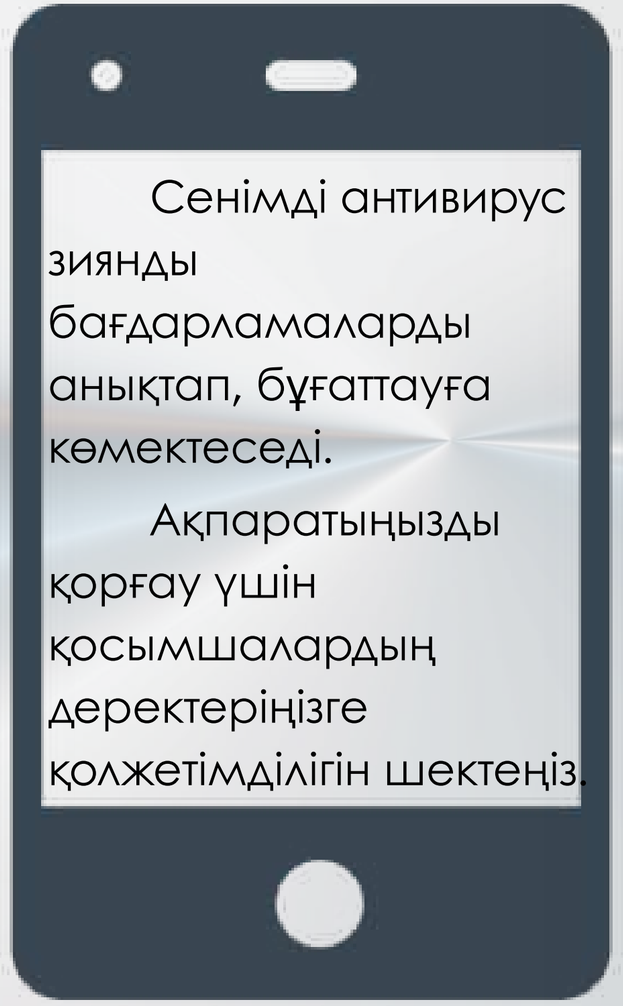
SOUTH KAZAKHYSTAN MEDICAL ACADEMY

ҚҰРЫЛҒЫЛАРЫМЫЗДЫ ҚОРҒАУДЫҢ НЕГІЗГІ ШАРАЛАРЫ:



Құрылғыны қорға үшін күрделі құпиясөз, PIN-код орнатыңыз және биометрияны пайдаланыңыз.

Қосымшаларды тек ресми көздерден жүктеңіз: Google Play немесе App Store-дағы қолданбалар қауіпсізірек.



Сенімді антивирус зиянды бағдарламаларды анықтап, бұғаттауға көмектеседі.

Ақпаратыңызды қорғау үшін қосымшалардың деректеріңізге қолжетімділігін шектеңіз.

Құрылғы ұрланған жағдайда оның орналасқан жерін бақылауға және деректерді қашықтан өшіруге мүмкіндік беретін функцияларды баптаңыз.

Маңызды деректерді үнемі сақтық көшірмеге сақтап отырыңыз — бұл ұрланған немесе бұзылған жағдайда жоғалтпауға көмектеседі.

2026

"Касперский зертханасы" халықаралық компаниясы 2024 жылғы 6 мамырда қазақстандықтарға маңызды мәлімдеме жасап, Telegram және WhatsApp–тағы фишингтік шабуылдар туралы ескертті

Алаяқтардың мақсаты–құпия деректерді ұрлау.

Жарты жылда 6,8 миллион алаяқтық ошағы – Қазақстанда танымал мессенджер нөмір телефоны бойынша алдау фабрикасына айналды!

Instagram желісінен деректердің таралғанда +77 және .kz көрсетілген: бұл Қазақстан азаматтарының деректері туралы екенін білдіреді.

Messenger

Іс–тәжірибелер

Кибер сауаттылық ережелерін сақтау және қорғаныс шешімдерін қолдану пайдаланушыны жағымсыз алаяқтық жағдайлардан сақтайды

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

AITU – Қазақстандық ұлттық мессенджер!

WhatsApp орнына – ұлттық мессенджер Aitu

Президент Тоқаевтың ұлттық мессенджер туралы тапсырмасы

- **Қазақстан Президенті Қасым-Жомарт Тоқаев жасанды интеллектті дамыту мәселелері жөніндегі кеңесте маңызды тапсырма берді.**
- **Үкіметке азаматтардың дербес деректерімен барлық коммуникацияларды қорғалған ұлттық мессенджерге көшіру жүктелді.**
- **Қазіргі уақытта мұндай мәліметтер көбінесе халықаралық сервистер арқылы беріледі, бұл:**
  - **деректердің елден тысқары таралу қаупін,**
  - **ұлттық қауіпсіздікке байланысты тәуекелдерді арттырады.**
- **Мемлекет басшысы AITU отандық қосымшасы**
  - **деректерді қорғаудың қажетті деңгейін қамтамасыз ете алатынын,**
  - **мемлекеттік және азаматтық коммуникациялар үшін қауіпсіз платформа бола алатынын атап өтті.**

ЖАСАНДЫ ИНТЕЛЕКТ

SOUTH KAZAKHYSTAN
MEDICAL ACADEMY

CYBER HYGIENE

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Жасанды интеллект: мүмкіндіктер мен тәуекелдер

Жеке деректер қауіпсіздігі

Әлеуметтік және психологиялық әсер

Қателіктер мен жауапкершіліктің белгісіздігі

Алаяқтық және жалған ақпарат

Әлеуметтік тәуелділік

ЖИ күнделікті өмірдің бір бөлігіне айналуда, ол YouTube арнасындағы ұсынымдардан бастап, бизнес–үдерістерді автоматтандыруға дейін кездеседі. Бірақ пайдасымен қатар, зияны да бар, себебі деректердің ұрлануы, манипуляциялар, фейктер, корпоративтік қауіпсіздіктегі осалдықтар орын алуда.

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

ЖИ пайдаланған кездегі ықтимал қауіптер

Қауіпсіздік қатері – ЖИ жүйелеріндегі осалдықтар хакерлер үшін жаңа шабуылдар жасау мүмкіндігін береді.

Байланыссыз шешімдер – Кейде ЖИ адамның контекстін дұрыс түсінбегендіктен қате немесе әділетсіз шешімдер шығарады.

Deepfake–контентін генерациялау

ЖИ–мен күшейтілген фишинг және әлеуметтік инженерия

Промпттар арқылы осалдықтар

ЖИ–сервистері арқылы құпия деректерді жіберу

Жалған ақпарат беру

SOUTH KAZAKHYSTAN MEDICAL ACADEMY

1. Жеке деректеріңізді немесе корпоративтік деректерді ашық нейрожелілерге ешқашан енгізбеңіз.

2. АТ–бөлімі ұсынған, тексерілген АТ–құралдарын ғана пайдаланыңыз.

3. ЖИ–ден алынған барлық ақпаратты ресми дереккөздер арқылы тексеріңіз.

4. Корпоративті ортада ЖИ пайдалану регламенті болуы тиіс: қандай деректерге рұқсат етілген, қандай әрекеттер АҚ бөлімімен келісуді талап етеді?

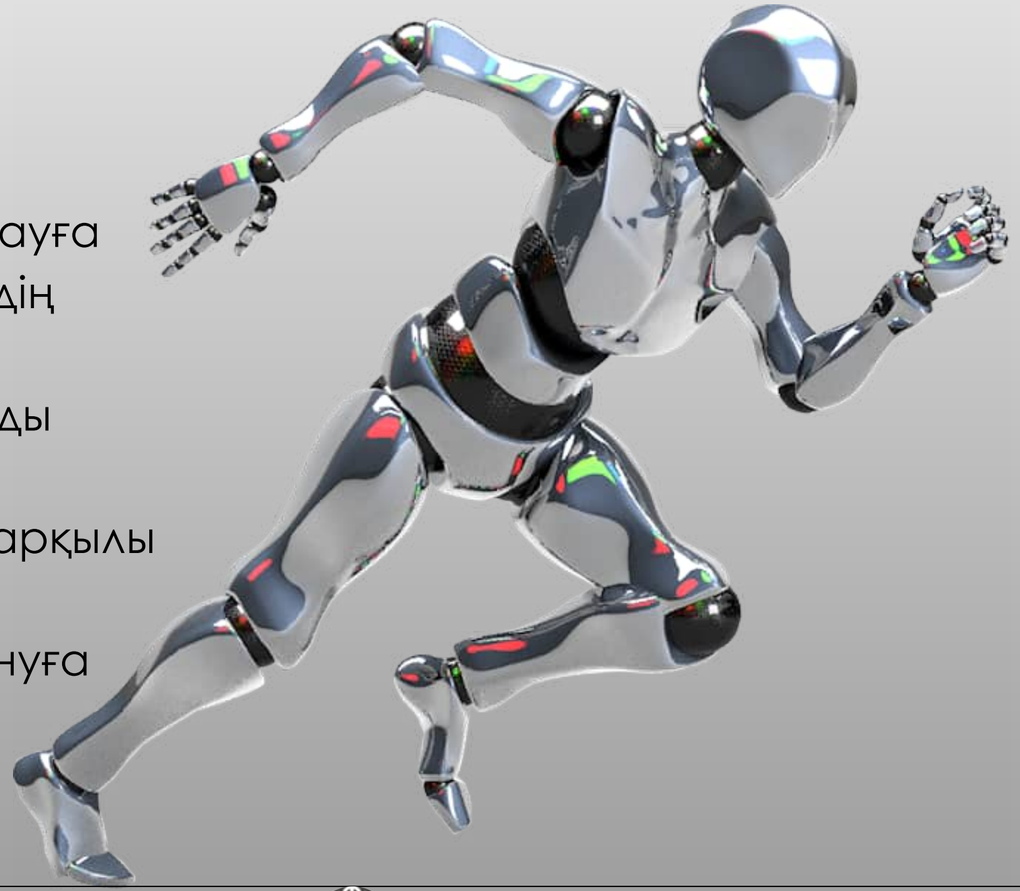
5. Дауыстарға, видеоларға және хаттарға тексермей, сенбеңіз, әсіресе «жедел ақша аудару» талап етілетін дауыстарға, хаттарға, бейнелерге сенбеңіз.

ЖИ-мен жұмыс жасағанда қалай қорғану қажет?

ЖИ-мен не жасауға болады, не жасауға болмайды? (шағын гайд)

✅ БОЛАДЫ:

a. Иесіз деректерді талдауға
b. Идеяларды, мәтіндердің үлгітүрлерін, сезімтал деректері жоқ кодтарды генерациялауға
c. Қауіпсіздігін бақылау арқылы ЖИ-ң корпоративтік нұсқаларын пайдалануға



❌ БОЛМАЙДЫ:

a. ЖИ-ге келісім-шарттарды, дербес деректерді ішкі аналитиканы көшіруге
b. Шешімдерді верификациясыз, автоматты түрде қабылдау үшін ЖИ пайдалануға
c. Құпия бизнес-логикасы бар промпттарды енгізуге

АҚШАҢДЫ КӨРСЕТ

ҚАЗАҚСТАН ҰЛТТЫҚ БАНКІ

SOUTH KAZAKHSTAN MEDICAL ACADEMY

ҚАРЖЫЛЫҚ ҚАУІПСІЗДІК ЖӨНІНДЕГІ ЖЕТІЛІКТІК

АҚШАҢЫЗДЫ АЛАЯҚТАРДАН ҚАЛАЙ ҚОРҒАУҒА БОЛАДЫ!

2026

SOUTH KAZAKHSTAN MEDICAL ACADEMY

Қаржылық мәселелер

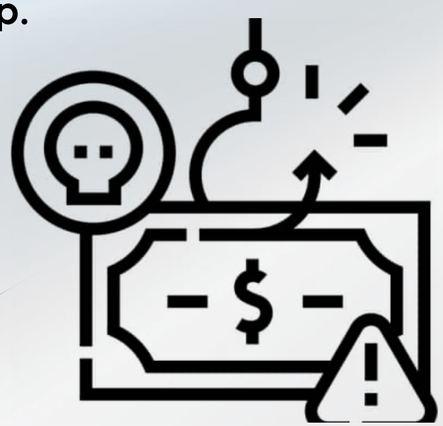
Фишинг

деректерді ұрлау үшін жасалған жалған сайттар мен хаттар.

Несие алаяқтығы

сіздің атыңыздан заңсыз несие рәсімдеу.

Скимминг



банкоматтарға арнайы құрылғылар орнатып, банк картасының деректерін көшіру.

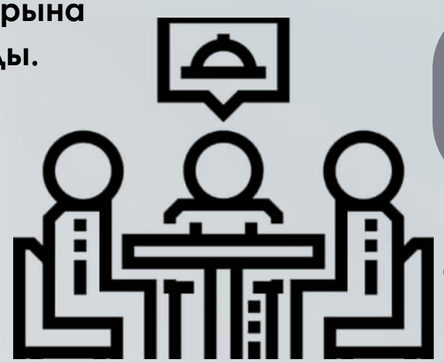
Деректер базаларын бұзу

Хакерлер клиенттердің карталары туралы ақпарат сақталатын компаниялардың деректер базаларына қолжетімдік алады.

Зиян келтіретін БЖ

Шпион-бағдарламалар онлайн-сауда жасаған кезде карталардың деректерін алып қою үшін компьютерлерде немесе смартфондарда орнатылады.

Дәмханада тағамның ақысын төлеу үшін картаны даяшыға беру.



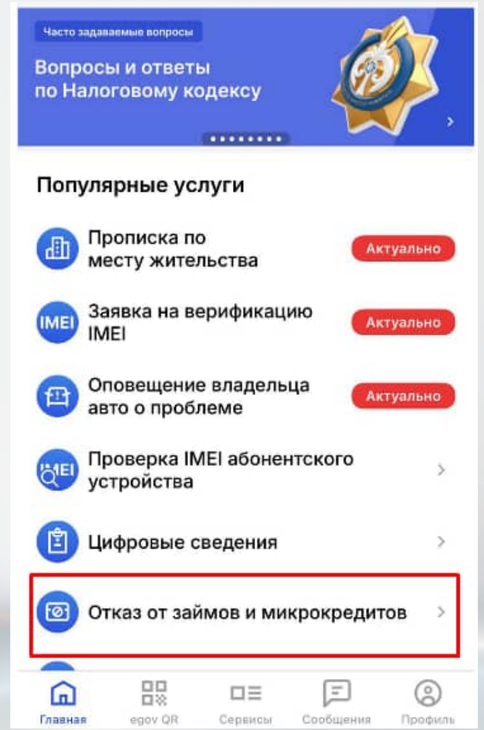
Банктік картаны үшінші тұлғаларға бермеңіз және әрдайым чек сұраңыз.

SOUTH KAZAKHSTAN MEDICAL ACADEMY

Қаржыны қауіпсіз қолдану бойынша

✅ Банкоматтарды мұқият тексеріңіз

Банкоматта скиммердің бар-жоғын қараңыз (картаны салатын жерде немесе пернетақтада күмәнді бөлшектер болмауы керек).



✅ eGov арқылы “Стоп-кредит” қызметін қосыңыз

Сіздің келісіміңізсіз несие рәсімдеуді шектеуге мүмкіндік береді.

✅ Қауіпсіз онлайн төлемдер жасаңыз

- Сатып алуды тек сенімді сайттарда жасаңыз.
- Интернет төлемдерге арналған лимиті бар жеке карта қолданыңыз

✅ Карта қолдану қауіпсіздігі

- 3D Secure — операцияны растау үшін SMS-код алуды қосыңыз.
- Екі факторлы аутентификация (2FA) — банк қосымшаларында қосымша қорғаныс орнатыңыз.

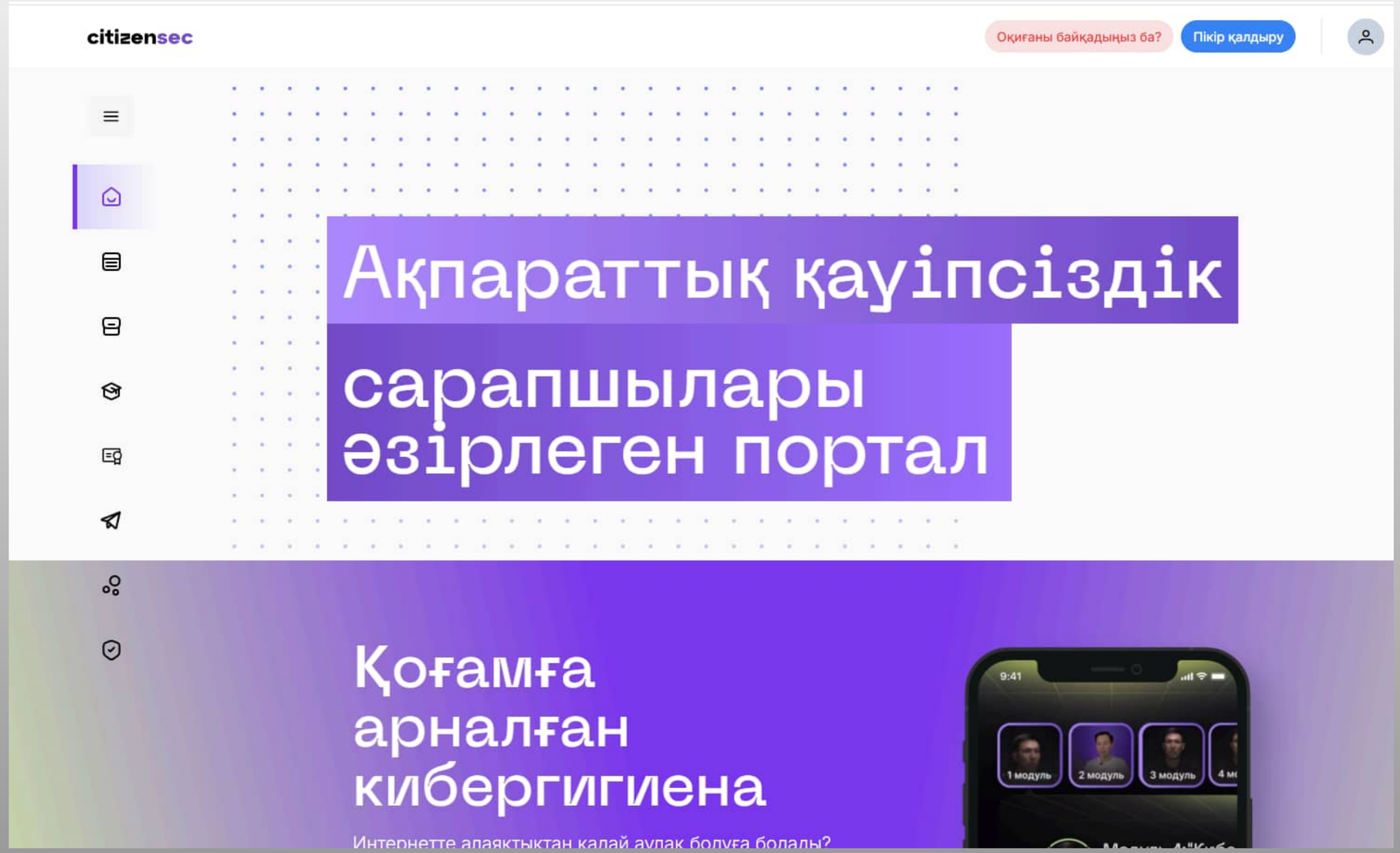
SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Пайдалы кеңестер

- 1.**Картаның деректерімен бөліспеңіз:** Егер алушының сенімді екеніне күдіктенсеңіз, онда картаңыздың нөмірін, әрекет ету мерзімін, CVV-кодын телефон, интернет немесе электрондық пошта арқылы хабарламаңыз.
- 2.**Сенімді сайттарды пайдаланыңыз:** Интернетте сауда жасаған кезде сайт қорғалған және сенімді екеніне көз жеткізіңіз. Әдетте сенімді сайттар https:// деп басталады және мекенжай жолағында құлыптың таңбасы болады.
- 3.**Шот бойынша үзінді көшірмелерді үнемі тексеріңіз:** Рұқсат етілмеген операциялар болмағанына көз жеткізу үшін банктік үзінді көшірмелерді жүйелі түрде тексеріңіз.
- 4.**SMS-хабарламаларды пайдаланыңыз:** Картаңыз бойынша барлық операциялар туралы уақтылы хабарлау үшін транзакциялар туралы SMS-хабарлауды қосыңыз.
- 6.**Картаның деректерін браузерде сақтамаңыз:** Картаңыздың деректерін веб-браузерлерде немесе сайттарда сақтауға жол бермеңіз

CITIZENSEC

SOUTH KAZAKHYSTAN MEDICAL ACADEMY



Ақпараттық қауіпсіздік сарапшылары порталы – бұл киберқауіпсіздік саласындағы мамандарға арналған онлайн платформа.

Киберқауіптерден бизнесіңізді пентест, осалдықтарды талдау, қауіпсіздік жүйесін құру және киберқауіпсіздік пен кибергигиена ережелерін үйрету арқылы қорғауға көмектеді.

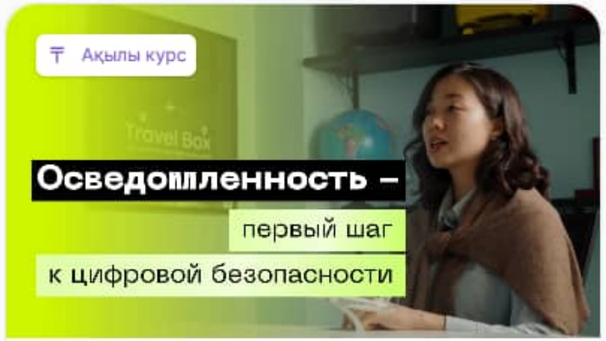
SOUTH KAZAKHYSTAN MEDICAL ACADEMY

Барлық курстар

Ұйымдар үшін кибергигиена (демо-нұсқа)

Бұл демо-нұсқа – корпоративтік және мемлекеттік секторға арналған қысқартылған курс.. Егер өзіңіз үшін қысқаша курсты көргіңіз келсе,...

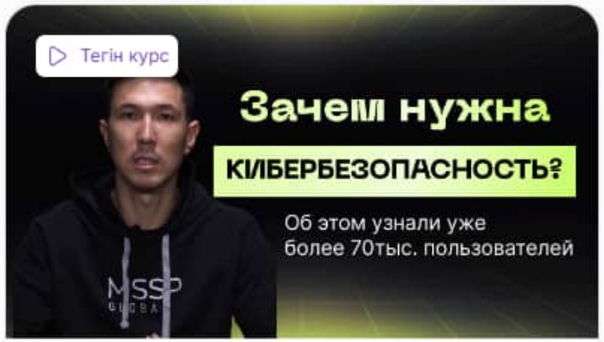
Өту



Корпоративтік қызметкерлерге арналған Кибергигиена

Бұл курс корпоративтік ұйымдардың қызметкерлеріне арнайы әзірленген және корпоративтік ортада кибергигиена деңгейін...

Өту



Кибергигиена

Цифрлық әлемде өзіңізді қалай қорғау керектігін, өзекті ақпарат, практикалық кеңестер мен

Жаңалық #Кибергигиена

Взлом Discord. Данные пользователей службы поддержки оказались в руках...

Платформа Discord сообщила о кибератаке, в результате которой часть данных пользователей оказалась украдена. Инцидент произошёл не из-...

@CitizenSec, 07-10-2025

Жаңалық #Қауіпсіздікке қатер төндірет

Новый вирус для Android -

В сети появился новый вредонос телефонов на Android под назван Его главная цель — кража личных

@CitizenSec, 18-08-2025

Арнайы шығарылым #Ақпараттық қауіпсіздік

Балаларды цифрлық әлемде қалай қорғауға болады: интернеттегі...

Қазіргі балалар цифрлық технологиялар дәуірінде өсуде — смартфондар, планшеттер, әлеуметтік желілер және онлайн ойындар олардың өмірінің...

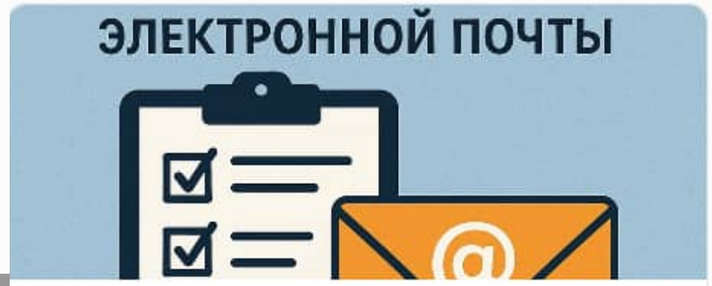
@citizensec, 30-05-2025

Мақала #Кибергигиена

Cookies, Super Cookies, Fi Мақсатты жарнама: бұлар

Cookies, super cookies, fingerprint жарнама: пайдаланушылардың ә бақыланады, қандай технологиял

@CitizenSec, 20-05-2025



Мақала #Кибергигиена

Полное руководство по ш диска: что это, зачем нуж

Шифрование диска — это важный защиты данных на вашем устрой

NomadGuard

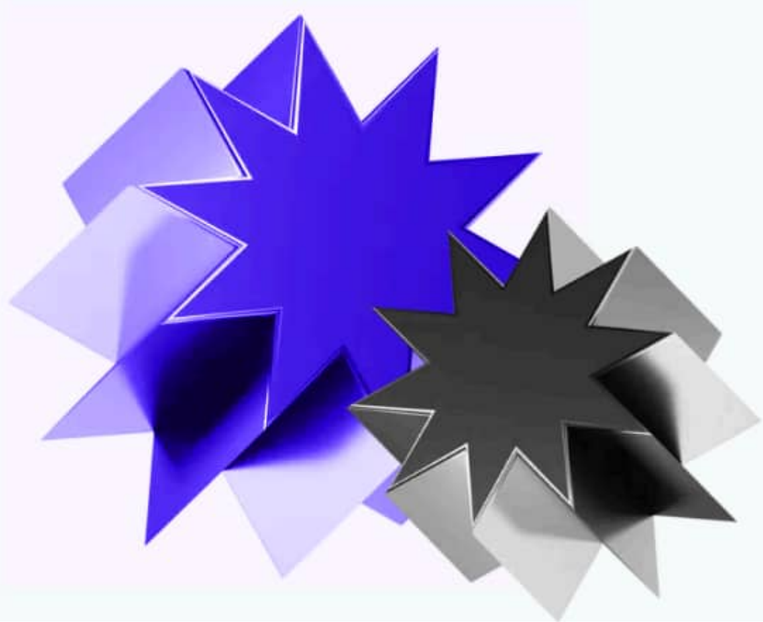
nomadguard.kz

SOUTH KAZAKHSTAN MEDICAL ACADEMY

NomadGuard | ҚАЗ | Жоба туралы | Мүмкіндіктер | Деректерді тексеру | Жаңалықтар | Кері байланыс | Кіру

Жоба туралы

Цифрландыру дәуірінде жеке деректерді қорғау маңызды. Nomad Guard — сіздің цифрлық қауіпсіздігіңізді қамтамасыз етудегі сенімді көмекшіңіз, цифрлық сауаттылықты дамыту бойынша бейне-жазбаларды ұсына отыра, сіздің жеке деректеріңіз интернетте жарияланғанда сізге уақытылы хабарлама жібереді.



Цифрлық сауаттылықты арттыру

Цифрлық мәдениетті қалыптастыру мақсатында, интернетте өзіңнің қауіпсіздігіңді қалай сақтауға болатыны жайлы бейне жазбалар

Жеке деректерді бақылау

Деректеріңіздің құпиялығы сақталғанын және алаяқтық мақсатта қолданбайтынын тексеріп отырыңыз

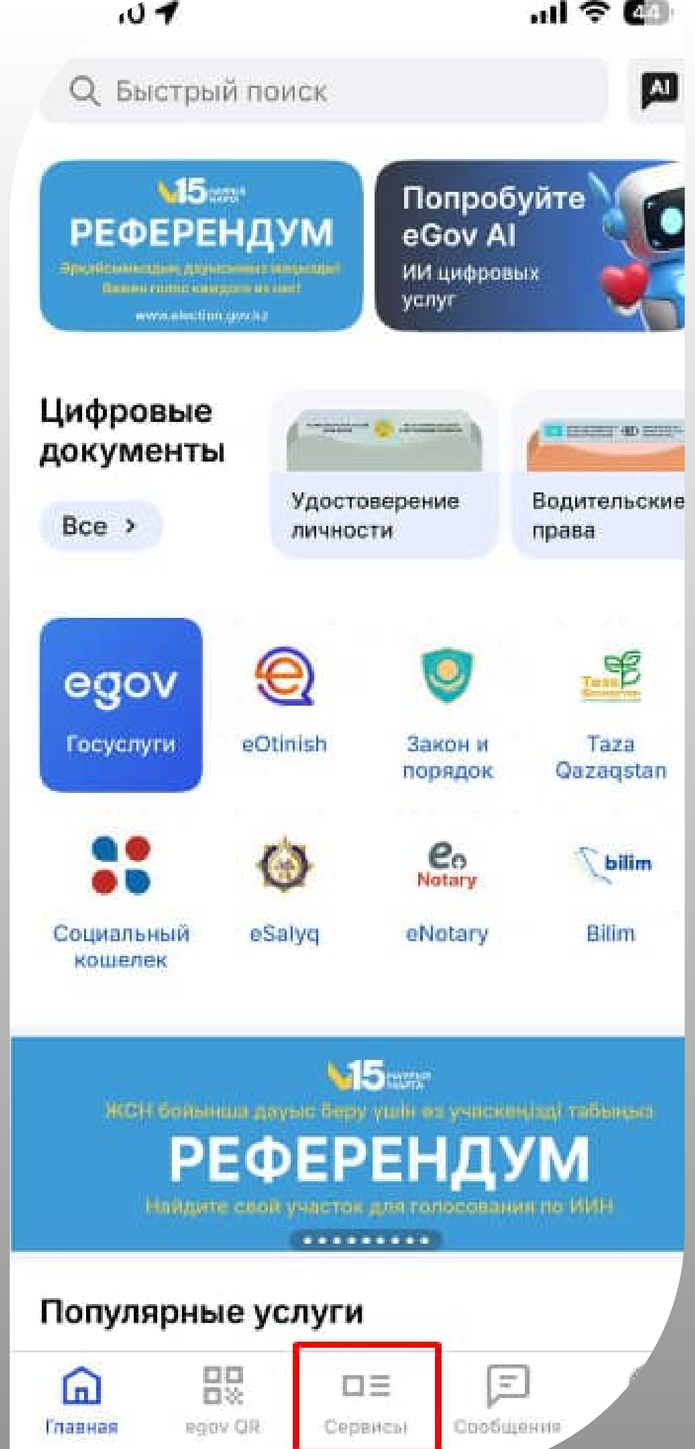
Жаңа жеке деректердің таралуы туралы хабарламалар

Деректеріңіздің қауіпсіздігін уақытында қамтамасыз ету үшін деректердің интернетте жария болуына қатысты хабарламаларды алып отырыңыз және барлық болған оқиғалардан хабардар болыңыз.

Киберқауіпсіздік туралы өзекті жаңалықтар

Киберқауіпсіздік әлеміндегі жаңалықтармен таныс болыңыз

Nomad Guard — Қазақстанда жеке деректер мен киберқауіпсіздік саласында қолданылатын жаңа қызмет және құрал. Ол әсіресе деректердің ағып кетуі мен онлайн алаяқтықтан қорғануға көмектесу үшін жасалған.



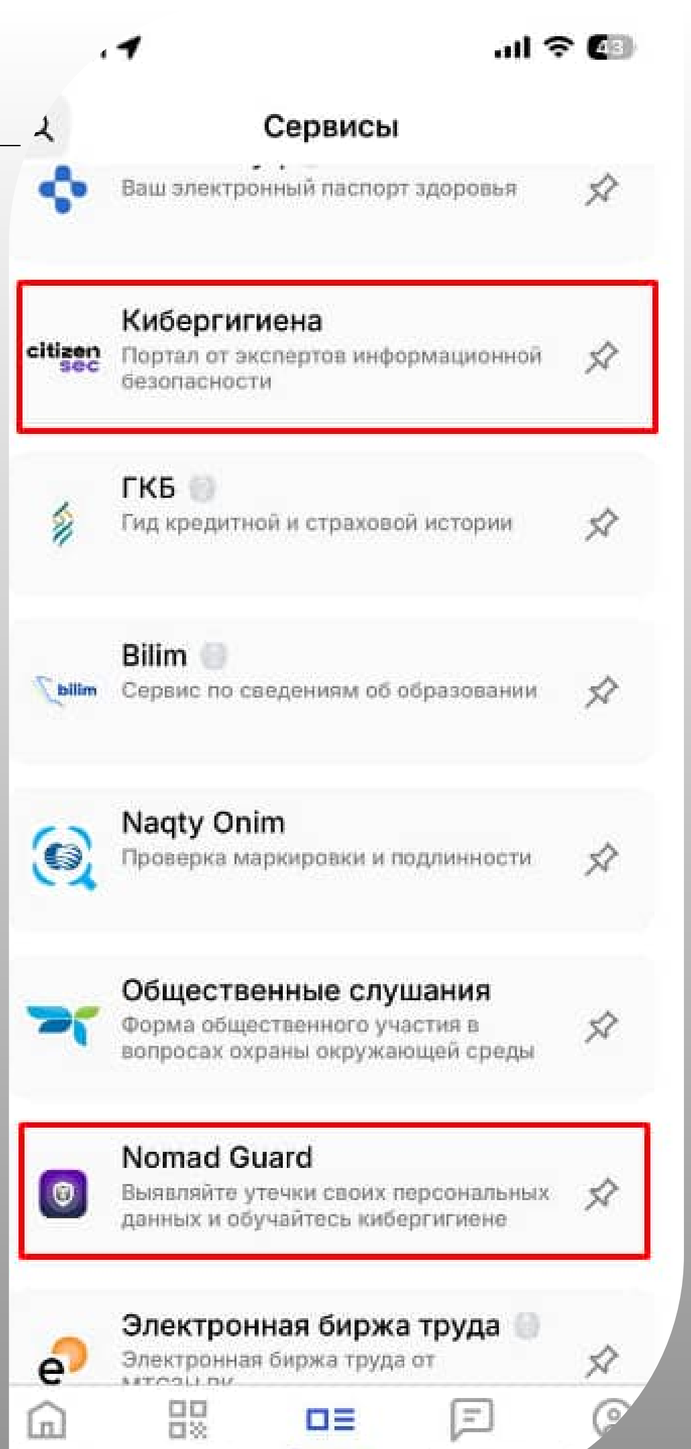
eGov Mobile мобильді қосымшасы арқылы қолжетімді Nomad Guard пен **Citizen**Sec – Қазақстан азаматтарының киберқауіпсіздігін арттыруға бағытталған сервистер.

🔐 CitizenSec

CitizenSec – киберқауіптер туралы хабарлау және алдын алу құралы.

🛡️ Nomad Guard

Nomad Guard – жеке деректердің интернетке ағып кетуін тексеруге арналған қызмет.



SOUTH KAZAKHSTAN
MEDICAL ACADEMY

Назарларыңызға рахмет!

(87252) 39-57-57, вн: 1010

skma.edu.kz

s.arynbayev@skma.edu.kz

г. Шымкент, пл. Аль-Фараби, 1.

Қорытынды

Кибергигиена – цифрлық қауіпсіздіктің негізгі тірегі. Қазіргі заманда жеке деректерді қорғау, күмәнді сілтемелерге өтпеу, сенімді құпиясөз қолдану және ақпаратты жауапкершілікпен тарату – әр азаматтың міндеті.

Сондықтан әрқайсымыз цифрлық ортада саналы әрекет етіп, жеке мәліметтерімізді қорғауға ерекше мән беруіміз қажет. Кибергигиена – қауіпсіз болашақтың кепілі.

Presented By: SABYRZHAN ARYNBAYEV
CYBERSECURITY AND INFORMATION SYSTEMS PROTECTION SPECIALIST