әл-Фараби атындағы Қазақ ұлттық университеті
География және табиғатты пайдалану факультеті
Рекреациялық география және туризм кафедрасы

4-дәріс

Кәсіпорын сатылымының цифрлық инфрақұрылымы және қонақ деректерін қорғау

Қонақ үй және туристік бизнестегі
ақпараттық технологиялар; ID 102602



ДӘРІСКЕР

Елдар Нұрұлы
Аға оқытушы, аға ғылыми
қызметкер, PhD Candidate

ДӘРІСТІҢ МАҚСАТЫ

Дәрістен кейін білім алушы

1. **Брондау деректерінің жолын түсіндіреді**
   браузерден қонақ үйдің базасына дейін
2. **Жүйелер қалай байланысатынын ажыратады**
   API, JSON, webhook, арналар менеджері
3. **Деректер қай жерде бұзылатынын анықтайды**
   синхрондау, хабарлама, ескі құжат
4. **Қорғау механизмдерін атайды**
   шифрлау, хеш, токен, екі факторлы кіру
5. **Шабуылдың техникалық жолын таниды**
   бақылаушы пиксель, фишинг, ClickFix

БҮГІНГІ ЖАҒДАЙ

Бір брондаудың цифрлық жолы

Айару іссапармен Алматыға келеді. Қонақ үйді смартфонындағы ЖИ-ассистент арқылы брондайды.

Сабақ барысында

Осы бір брондаудың соңынан 12 станциядан өтеміз. 6 деректердің қалай жылыстайтынын, 6 олардың қалай қорғалатынын көрсетеді.



ЖОЛ КАРТАСЫ

Он екі станция, екі бөлім

1-бөлім · Деректер қалай жылыстайды

1 Батырма басылды

2 API

3 Арналар менеджері

4 Webhook

5 Төлем токені

6 Бот

2-бөлім · Деректер қалай қорғалады

7 HTTPS құлпы

8 Құпиясөз хеші

9 Бақылаушы пиксель

10 Фишинг

11 Екі факторлы кіру

12 Бұзылуды байқау

1-БӨЛІМ

Деректер қалай жылыстайды

Брондау батырмадан қонақ үйдің базасына дейін қалай жетеді



1-станция

«Брондау» батырмасын басқанда не болады

Браузер сұраныс жібереді: «мына күндерге бөлме бар ма?»

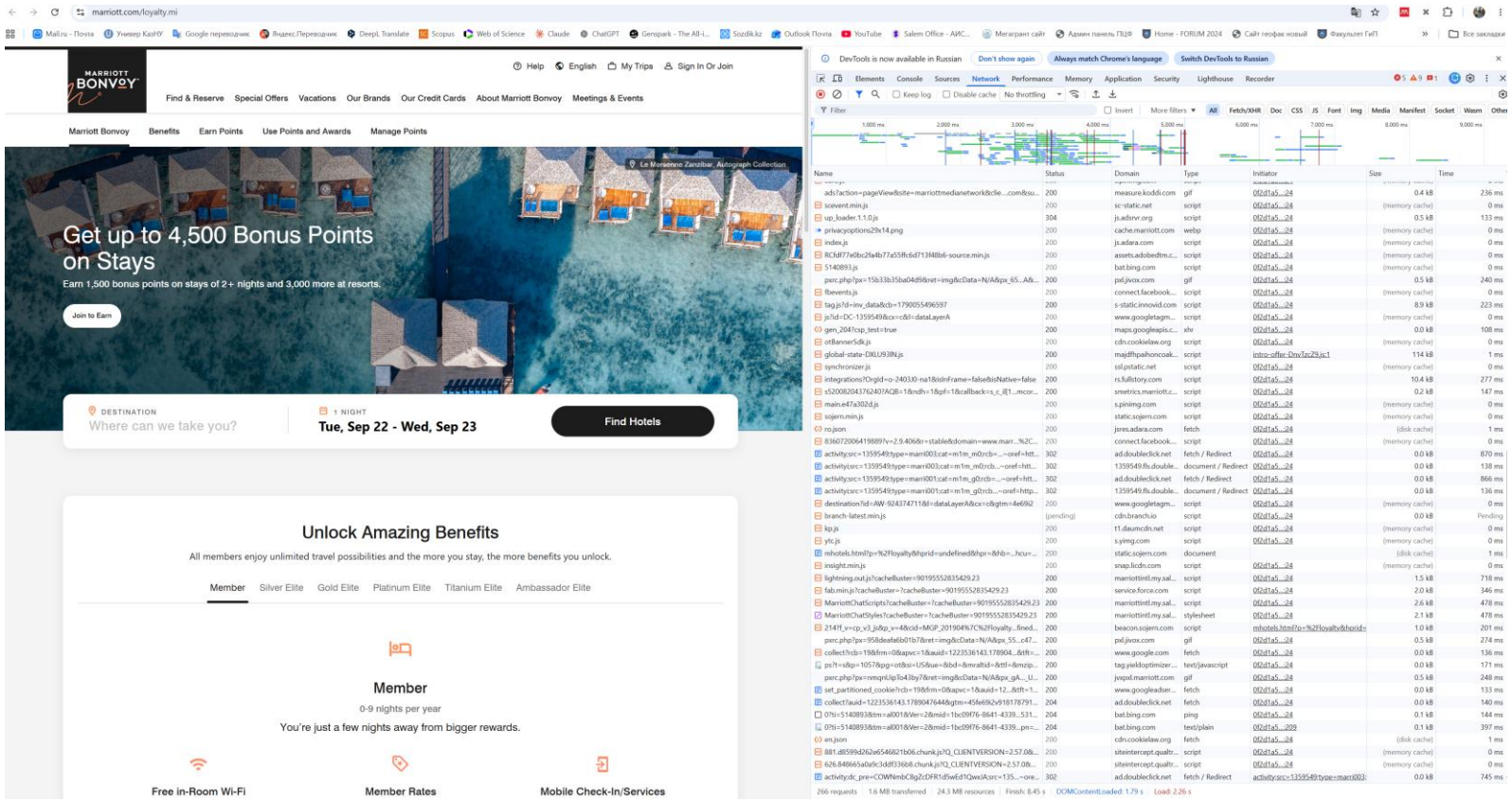
Сервер базадан тексереді

Жауап «бар, бағасы мынадай» деген деректер қайтады



Өзіңіз көріңіз

Chrome-да F12, Network қойындысы. Бетті жаңартсаңыз, барлық сұраныс тізіліп шығады.



Network қойындысын қалай оқу керек**:**

① **Name** – не сұралды: файл, сурет, команда
② **Status** – 200 берілді, 302 әрі қарай жіберілді
③ **Domain** – сұраныс кімге кетті. Ең маңызды бағаң
④ **Type** – script бағдарлама, gif көрінбейтін пиксель
⑤ **Төменгі жол** – 266 сұраныс, 8,45 секунд

marriott.com-нан басқаның бәрі бөгде компания

2-станция

Жүйелер бір-бірімен келісілген тілде сөйлеседі

API (Application Programming Interface): бір бағдарлама екіншісінен деректі қалай сұрайтынын анықтайтын ереже. Сайт, брондау алаңы, PMS және төлем жүйесі бір-бірімен осылай байланысады.

Мейрамханадағы мысал

Сіз ас үйге кірмейсіз. Даяшыға мәзірдегі тағамды айтасыз, ол алып келеді. Даяшы осы жерде API рөлінде.

Мәзір

API-да сұрауға болатын нәрселер алдын ала жазылған. Мәзірде жоқ тағамды сұрай алмайсыз.

Жауап

Жауап белгілі бір пішімде келеді. Көбіне бұл JSON (JavaScript Object Notation).

Бір брондау 5-6 API арқылы өтеді. Біреуі кешіксе, деректер сәйкес келмей қалады.

Брондау жүйе ішінде осылай көрінеді

```
{
  "guest": "Aiaru S.",
  "room_type": "Standard",
  "check_in": "2040-10-12",
  "check_out": "2040-10-14",
  "price_total": 56000,
  "currency": "KZT",
  "channel": "website",
  "payment_token": "tok_8f3kQ2",
}
```

Оқу мысалы. Нақты жүйенің деректері емес.

Кілт пен мән

Сол жақта не туралы екені, оң жақта мәні. Мысалы, check_in кілті, 2040-10-12 мәні.

Назар аударыңыз

Карта нөмірі жоқ. Оның орнында payment_token тұр. Неге екенін 5-станцияда көреміз.

3-станция

Бір жазба бірден бес алаңға тарайды





Синхрондау кешіксе

Соңғы бөлмені екі адам екі алаңнан бір мезетте брондайды.

Сұрап отырмау, хабарламаны күту

Сұрау тәсілі

PMS брондау алаңынан әр бес минут сайын «жаңа брондау бар ма?» деп сұрайды. Жүз рет сұрап, бір рет жауап алуы мүмкін.

Webhook тәсілі

Брондау түскен сәтте алаң PMS-ке өзі хабар жібереді. Сұрау жоқ, кешігу жоқ.

(Webhook – бұл нақты уақыттағы HTTP сұраулары арқылы сыртқы жүйелерге оқиғалар туралы автоматты түрде хабарлау механизмі).

Күнделікті мысал

Курьерді күтіп, терезеден әр бес минут қарау бірінші тәсілге ұқсайды. Курьер келгенде өзі қоңырау шалуы webhook-қа ұқсайды.

ТОКЕНИЗАЦИЯ · КАРТА НӨМІРІН АЛМАСТЫРУ

5-станция

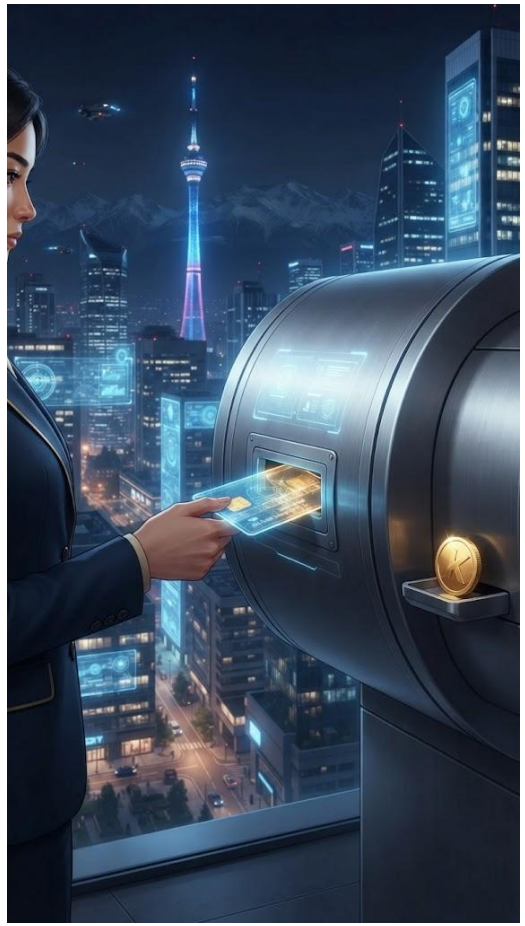
Карта нөмірі таңбаға айналады

```
4400 1234 5678 9010
```

↓ төлем шлюзі

```
tok_8f3kQ2
```

Қонақ үй тек таңбаны сақтайды. Таңба ұрланса, одан карта нөмірін қалпына келтіру мүмкін емес.



Келесі станция: бот жауапты қайдан табады

БОТ ҚАЛАЙ ЖАУАП ТАБАДЫ

6-станция

Gem сіздің құжатыңыздан іздейді

Сұрақ

«Заезд қашан?»

Іздеу

бот жүктелген құжаттан сәйкес жерді табады

Жауап

табылған мәтін негізінде жауап құрады

Құжат дұрыс

Бот сайтпен бірдей жауап береді.

Құжат ескі

Бот ескі деректі сенімді түрде айтады.

Семинарда сіздің ботыңыз төртінші дереккөз ретінде тексеріледі.

САЙТ ЖЫЛДАМДЫҒЫ

Google сайтты үш өлшеммен бағалайды

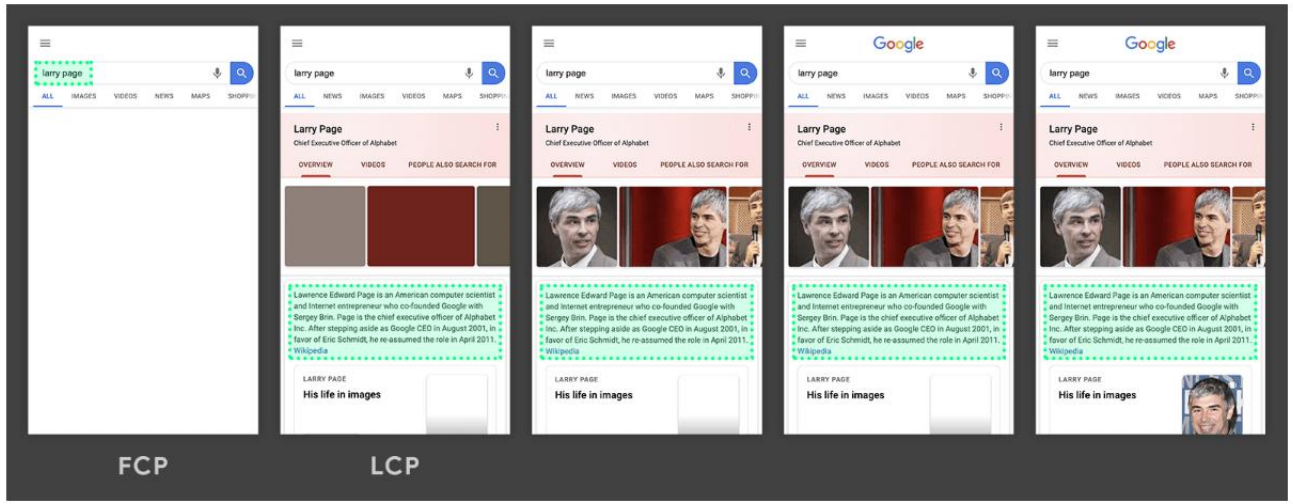
Көрсеткіш	Нені өлшейді	Жақсы	Нашар
LCP (Largest Contentful Paint)негізгі мазмұнның көріну уақыты: беттің басты суреті немесе тақырыбы қанша секундта шығады.	Негізгі мазмұн қанша уақытта көрінеді	2,5 с дейін	4 с артық
INP (Interaction to Next Paint)әрекетке жауап беру уақыты: батырманы басқаннан кейін бет қаншалықты тез жауап береді.	Батырманы басқанда жауап жылдамдығы	200 мс дейін	500 мс артық
CLS (Cumulative Layout Shift) *беттің жылжуы: жүктелу кезінде элементтер қаншалықты секіреді.*	Жүктелгенде бет қаншалықты секіреді	0,1 дейін	0,25 артық

Бір маңызды өзгеріс

2024 жылғы 12 наурыздан бастап INP ескі FID (First Input Delay) көрсеткішінің орнын басты. Бағалау нақты қонақтардың 75 пайызы бойынша жүргізіледі.

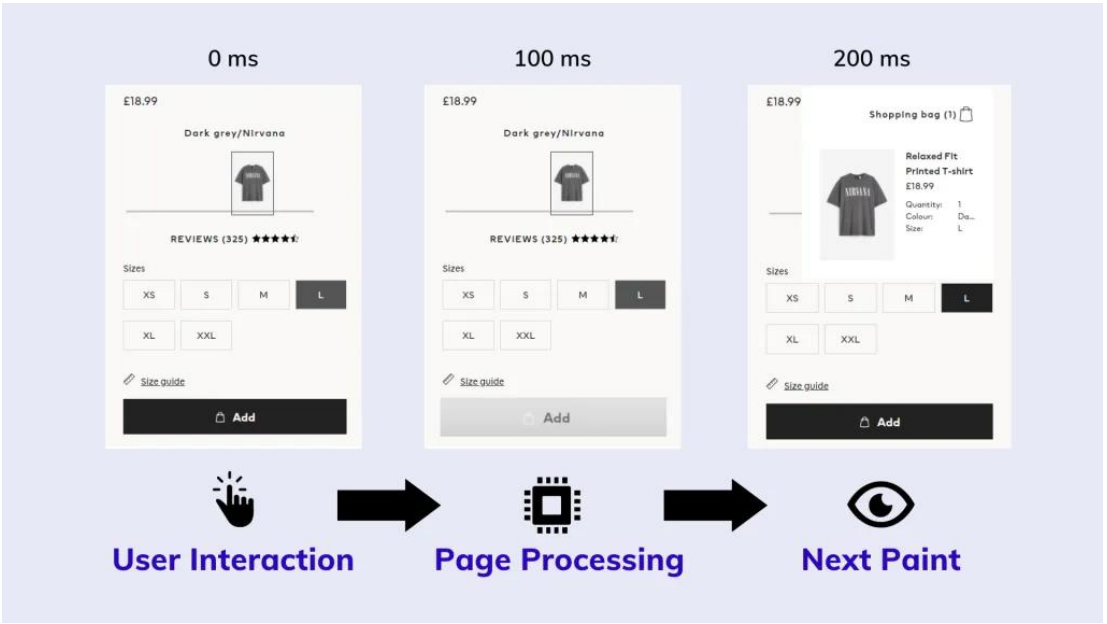
Дереккөз: Google web.dev, Web Vitals

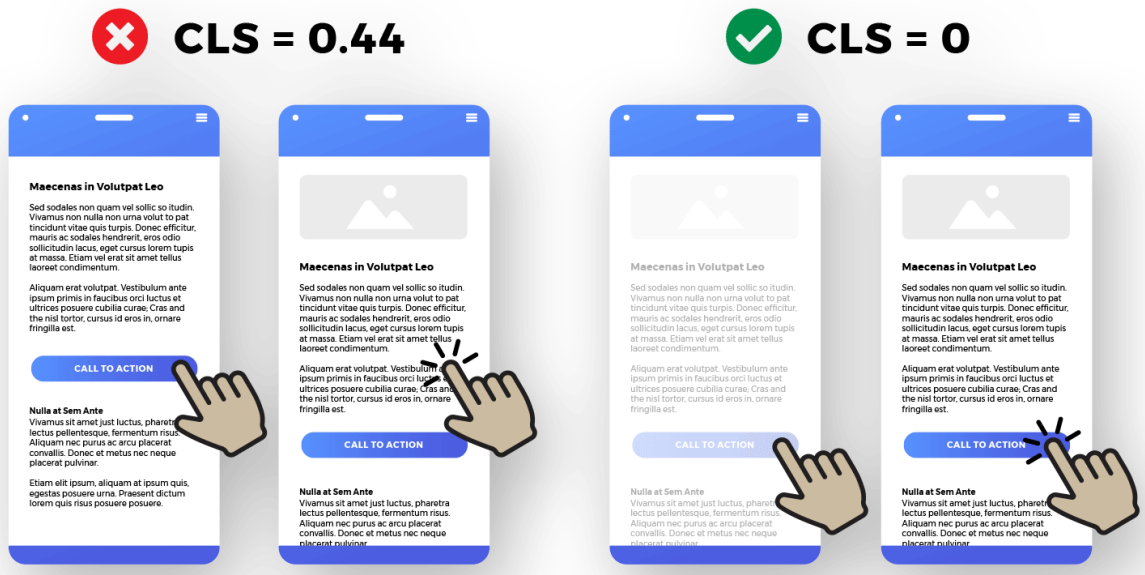
LCP (Largest Contentful Paint)



Хронология LCP с сайта google.com.

INP (Interaction to Next Paint)





CLS (Cumulative Layout Shift)

1-БӨЛІМНІҢ ҚОРЫТЫНДЫСЫ

Брондау алты жүйеден өтті. Әр жүйеде көшірмесі қалды

Не білдік

Брондау API арқылы жүйеден жүйеге өтеді. Арналар менеджері таратады, webhook хабарлайды, токен картаны жасырады.

Енді сұрақ

Брондау өткен әр жүйе оның көшірмесін сақтайды. Бұл көшірмелерді кім және қалай қорғайды?

Деректер қай жерде сақталса, сол жерден ұрлануы мүмкін.

2-БӨЛІМ

Деректер қалай қорғалады

Деректер қай жерде осал және оларды не қорғайды



Мекенжай жолындағы құлып не істейді

http

Ашық хатқа ұқсайды. Жолдағы кез келген адам оқи алады.

https

Жабық конвертке ұқсайды. Браузер мен сервер арасы шифрланған.



Шектеуі

Құлып жолды қорғайды, бірақ сайттың өзі адал екенін дәлелдемейді. Фишинг сайттарында да құлып болады.

ХЕШ · ҚҰПИЯСӨЗДІҢ САУСАҚ ІЗІ

8-станция

Дұрыс жүйе құпиясөзіңізді білмейді

```
Айару123   →   SHA-256   →   79b79b7c1bb31d9e...
```

Бір бағытты

Хештен құпиясөзді кері шығару мүмкін емес.

Кіру кезінде

Енгізген құпиясөз қайта хештеледі және сақталған хешпен салыстырылады.

Қате тәсіл

Құпиясөзді ашық сақтау. Базасы ағып кетсе, барлық құпиясөз бірден ашылады.

Мысал SHA-256 алгоритмімен жасалған. Құпиясөзді сақтау үшін OWASP әдейі баяу жұмыс істейтін арнайы алгоритмдерді ұсынады.

Дереккөз: OWASP Password Storage Cheat Sheet

БАҚЫЛАУШЫ ПИКСЕЛЬ

9-станция

Көрінбейтін нүкте деректерді алып кетеді

1. Сайтқа көлемі бір нүктедей көрінбейтін сурет орнатылады
2. Бетті ашқанда браузер оны бөгде сервердан жүктейді
3. Сұраныспен бірге қай бет, қай құрылғы, қайдан келді деген мәлімет кетеді



Ірі желінің бір бетінде: 89 сұраныс, 9 бөгде алушы, олардың бірі сеансты жазады.

Дереккөз: Chrome әзірлеуші құралдары, 2026 жылғы қыркүйек

СЕАНСТЫ ЖАЗУ

9-станция

Сайт сіздің әр қимылыңызды видеоға жазуы мүмкін

Не жазылады	Қалай қолданылады
Тінтуір қозғалысы	Қонақ қай жерде тоқтап, ойланды
Басу мен айналдыру	Қай батырма жұмыс істемеді
Форманы толтыру	Қай өрісте қонақ брондаудан бас тартты

Екі жақты құрал

Сайтты жақсарту үшін пайдалы. Бірақ дұрыс бапталмаса, формаға енгізілген деректер де жазылып қалуы мүмкін. Семинарда Blacklight мұны тексереді.

Келесі станция: шабуыл жүйеге емес, адамға жасалғанда

ФИШИНГ

10-станция

Шабуыл алаңға емес, қонақ үйдің қызметкеріне жасалды

1

Хат

Қызметкерге брондау алаңынан келгендей хат: жаман пікір, қонақтың сұрауы

2

Зиянды бағдарлама

Қызметкер нұсқаулықты орындайды, компьютерге құпиясөз ұрлағыш түседі

3

Кабинет

Шабуылдаушы қонақ үйдің кабинетіне кіріп, нақты брондауларды көреді

4

Қонаққа хат

Қонаққа оның нақты деректерімен «төлемді растаңыз» деген хат кетеді



Дереккөз: Microsoft Security Blog, 13.03.2025 (Storm-1865 тобы)

10-станция

Сайт буферге жасырын команда көшіреді

Жалған тексеру

«Робот емес екеніңізді растаңыз» терезесі

Жасырын көшіру

Батырманы басқанда буферге команда көшіріледі

Нұсқаулық

Win+R, Ctrl+V, Enter

Нәтиже

Команданы адамның өзі іске қосады

Ешбір сайт сізден пернетақтамен команда енгізуді сұрамайды.

Мұндай нұсқаулықты көрсеңіз, терезені жабыңыз және IT маманына хабарлаңыз.

Дереккөз: Microsoft Security Blog, 13.03.2025

2FA · ЕКІ ФАКТОРЛЫ КІРУ

11-станция

Ұрланған құпиясөз жалғыз өзі жеткіліксіз

Бірінші фактор

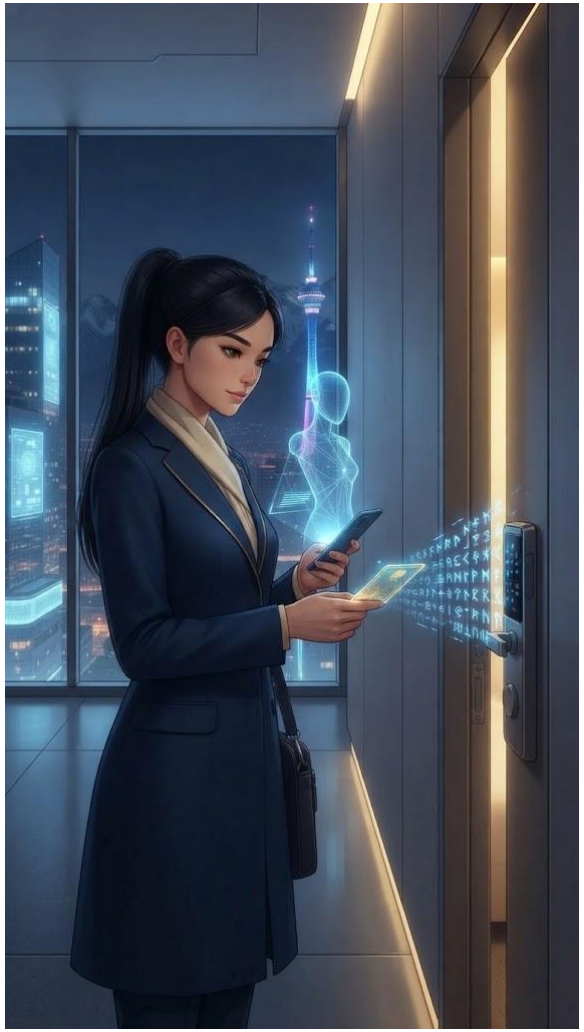
Сіз білетін нәрсе: құпиясөз.

Екінші фактор

Сізде бар нәрсе: телефондағы код.

```
482 915   ·   30 секундтан кейін жаңарады
```

Код уақыт пен құпия кілт негізінде есептеледі. Ол ұрланған құпиясөзден қорғайды, бірақ жалған беттен қорғамайды.



Дереккөз: RFC 6238, TOTP: Time-Based One-Time Password Algorithm

БҰЗЫЛУДЫ БАЙҚАУ

12-станция

Шабуыл төрт жыл бойы неге көрінбеді

2014

Starwood жүйесіне шабуыл

2016

Marriott Starwood-ты сатып алды

2018

Шабуыл тек осы жылы байқалды

2020

Британия реттеушісі 18,4 млн £ айыппұл салды

Не ұрланды

339 млн қонақ жазбасы. Оның ішінде 5,25 млн шифрланбаған төлқұжат нөмірі.

IT сабағы

Жүйе журналдарын ешкім бақыламаса, шабуыл жылдар бойы байқалмайды. Қорғау бұзылуды байқаудан басталады.

Дереккөз: UK ICO, 30.10.2020; Marriott International ресми хабарламасы

Marriott International Update on Conclusion of UK ICO Investigation into



<< Back

BETHESDA, MD – OCTOBER 30, 2020 – Marriott International, Inc. (NASDAQ: MAR) ("Marriott") acknowledges the decision issued today by the UK Information Commissioner's Office (the "ICO"), which brings an end to the UK and EU regulatory investigation of the Starwood reservations database incident reported by Marriott in November 2018.

The decision includes a fine of £18.4 million. Marriott does not intend to appeal the decision, but makes no admission of liability in relation to the decision or the underlying allegations. As the ICO acknowledges, Marriott cooperated fully throughout the investigation.

Marriott deeply regrets the incident. Marriott remains committed to the privacy and security of its guests' information and continues to make significant investments in security measures for its systems, as the ICO recognizes. The ICO also recognizes the steps taken by Marriott following discovery of the incident to promptly inform and protect the interests of its guests.

Marriott wants to reassure guests that the incident and the ICO's decision involved only Starwood's separate network, which is no longer in use.

About Marriott International

Marriott International, Inc. (NASDAQ: MAR) is based in Bethesda, Maryland, USA, and encompasses a portfolio of more than 7,400 properties under 30 leading brands spanning 135 countries and territories. Marriott operates and franchises hotels and licenses vacation ownership resorts all around the world. The company offers Marriott Bonvoy™, its highly-awarded travel program. For more information, please visit our website at www.marriott.com, and for the latest company news, visit www.marriottnewscenter.com. In addition, connect with us on Facebook and @MarriottIntl on Twitter and Instagram.

Marriott may post updates about the reservations database incident and other matters on its investor relations website at www.marriott.com/investor or Marriott's news center website at www.marriottnewscenter.com. Marriott encourages investors, the media, and others interested in the company to review and subscribe to the information Marriott posts on these websites, which may be material. The contents of these websites are not incorporated by reference into this announcement or any report or document Marriott files with the SEC, and any references to the websites are intended to be inactive textual references only.

ЖАЛҒАН БЕТ · АРАДАҒЫ ШАБУЫЛ

Телефондағы кодты да ұрлауға болады

1. Жалған бет

Нақты сайттың дәл көшірмесін көрсетеді

2. Сіз енгізесіз

Құпиясөз бен телефондағы кодты

3. Бет жібереді

Екеуін де нақты сайтқа сол сәтте

4. Сеанс ұрланады

Шабуылдаушы ашылған сеанспен кіреді

Мұндай бетке төтеп бермейді

SMS арқылы келген код

Қосымшадағы 6 таңбалы код

Телефонға келген «растау» хабарламасы

Төтеп береді

Кіру кілттері (passkeys) және FIDO2 физикалық кілттері. Олар сайттың мекенжайына байланған, сондықтан жалған бетте жұмыс істемейді.

Дереккөз: CISA, фишингке төзімді көп факторлы аутентификация жөніндегі нұсқаулық

ҚОНАҚ ҮЙ ДЕҢГЕЙІНДЕ

Кәсіпорын ертеңнен бастап енгізе алатын алты ереже

1 Кері қоңырау

Құпиясөзді қалпына келтіру тек бұрыннан белгілі нөмірге кері қоңырау шалғаннан кейін

2 Бөлек компьютер

Брондау алаңының кабинеті ашылатын компьютерде пошта ашылмайды

3 Әркімге жеке логин

Бір құпиясөзбен бүкіл ауысым жұмыс істемейді. Кеткен қызметкердің кіруі сол күні жабылады

4 Ауысым соңында шығу

Кабинеттен шығу, жұмыс браузерінде құпиясөз сақтамау

5 QR-кодты тексеру

Үстелдегі және бөлмедегі кодтың үстіне бөтен стикер жабыстырылмағанын қарау

6 Кіру кілттері

Мүмкін болса, алаң кабинетіне кіру кілті немесе FIDO2 кілті арқылы кіру

1-ереже неге маңызды: MGM Resorts 2023 жылғы шабуылдан шамамен 100 млн доллар шығын көрді. Шабуылдаушылардың өз сөзі бойынша, бәрі қолдау қызметіне телефон қоңырауынан басталған.

Дереккөз: MGM Resorts, SEC-ке 8-K есебі (05.10.2023); FBI IC3, PSA 18.01.2022; CISA

ӨЗІҢІЗ ҮШІН

Бүгін кешке жасауға болатын бес әдет

1

Кіру кілтін қосу

Google аккаунтында құпиясөздің орнына кіру кілтін баптаңыз

2

Белсенді сеанстарды қарау

Google мен Telegram-да қай құрылғыда кіргеніңізді тексеріп, бөтенін жабыңыз

3

Telegram бұлтты құпиясөзі

Екі кезеңді тексеруді қосыңыз: SMS кодынан бөлек тағы бір құпиясөз

4

SMS орнына қосымша

SMS кодты SIM картаны алмастыру арқылы ұрлауға болады. Код генераторы немесе кіру кілті сенімдірек

5

Ағып кетуді тексеру

haveibeenpwned.com поштаңыз қай деректер ағып кетуінде болғанын көрсетеді

Дереккөз: FBI IC3, SIM картаны алмастыру схемалары туралы PSA, 08.02.2022

ЗАҢ РАМКАСЫ

Технологияның үстінде тұрған талаптар

Келісім	Деректерді жинау үшін қонақтың келісімі керек
Ең аз көлем	Тек мақсатқа қажеттісін жинау
Сақтау орны	ҚР азаматтарының деректері бар база Қазақстан аумағында болуы тиіс
Шекара арқылы беру	Шетелге беруге жеке талаптар қойылған

Сақтау орны туралы талап сервер таңдауға тікелей әсер етеді: шетелдік бұлтқа бәрін сала салуға болмайды.

Дереккөз: ҚР № 94-V Заңы, 12-бап 2-тармақ, 16-бап. Соңғы өзгерістер 16.09.2025 күшіне енді

1-ИНТЕРАКТИВ · 5 МИНУТ

Қай механизм шабуылды тоқтатар еді?

А Кафедегі ортақ Wi-Fi арқылы біреу брондау формасын оқып алды

Ә Қонақ үйдің базасы жылыстап кетті, бірақ құпиясөздерді ешкім ашпады

Б Қызметкердің құпиясөзі ұрланды, бірақ электронды кабинетке кіру мүмкін болмады

В Базадан карта деректері табылды, бірақ олармен төлеу мүмкін емес

Әр жағдайға бір механизмді атаңыз: HTTPS, хеш, екі факторлы кіру немесе токен.

1-ИНТЕРАКТИВ · ТАЛДАУ

Әр механизм өз шабуылын тоқтатады

	Механизм	Неге
А	HTTPS	Құлыпсыз сайтта форма ашық жолмен кетеді
Ә	Хеш	Базада құпиясөз емес, хеш сақталған
Б	Екі факторлы кіру	Құпиясөз бар, бірақ телефондағы код жоқ
В	Токен	Базада карта нөмірі емес, таңба сақталған

Бір механизм барлық шабуылдан қорғамайды. Қорғау қабат-қабат құрылады.

ҚОРЫТЫНДЫ

Дәрістен нені есте сақтау керек

1. Брондау API арқылы жүйеден жүйеге JSON пішімінде өтеді
2. Қате көбіне екі жүйенің түйіскен жерінде туады
3. Карта нөмірінің орнына токен, құпиясөздің орнына хеш сақталады
4. Біз қараған ірі шабуылдар технологиядан емес, адамнан басталды
5. Қорғау бұзылуды байқаудан басталады



СЕМИНАРҒА ТАПСЫРМА

Цифрлық аудит: үш нысанды тексеру

Команда өз кәсіпорнын және екі бәсекелесін төрт станцияда тексереді. Нәтиже бір кестеге жиналып, әр нысанның цифрлық денсаулық индексі есептеледі.

1

Жылдамдық

PageSpeed Insights

2

Құпиялылық

Blacklight

3

Сәйкессіздік

сайт, алаң, карта, бот

4

Қорғау

тексеру парағы

Семинарға бот сілтемесін және кәсіпорынның брондау алаңындағы бетін дайындап келіңіз.

АКАДЕМИЯЛЫҚ АДАЛДЫҚ

Жасанды интеллектті пайдалану туралы декларация

Қолданылған құрал	Claude (Anthropic компаниясы). Иллюстрациялар: Gemini.
ЖИ не істеді	Дереккөздерді салыстыру; слайдтарды құрастыру; иллюстрацияларға промт жазу; мәтінді редакциялау.
Оқытушы не берді	Дәрістің тақырыбы мен құрылымы; мәтінін; сайттағы бақылаушыларды тексеру нәтижесі; интерактивтердің шарты.
Оқытушы нені тексерді	Әр факт бастапқы дереккөзбен салыстырылды; заң редакциясы ресми базадан тексерілді; әр сілтеме ашылды.

Дәрістің мазмұны мен дереккөздердің түпнұсқалығы үшін жауапкершілік дәріскерде.

Технологиялар мен заңнама

1 MDN Web Docs. HTTP. Mozilla. https://developer.mozilla.org/en-US/docs/Web/HTTP

2 Google. (2024). Web Vitals. web.dev. https://web.dev/articles/vitals

3 OWASP. Password Storage Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

4 M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). TOTP: Time-Based One-Time Password Algorithm (RFC 6238). IETF. https://datatracker.ietf.org/doc/html/rfc6238

5 Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V «Дербес деректер және оларды қорғау туралы» Заңы. https://adilet.zan.kz/kaz/docs/Z1300000094

Қауіпсіздік және құралдар

6 Microsoft Threat Intelligence. (2025, March 13). Phishing campaign impersonates Booking.com, delivers a suite of credential-stealing malware. https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/

7 Marriott International. (2020, October 30). Update on conclusion of UK ICO investigation into Starwood database security incident. https://marriott.gcs-web.com/news-releases/news-release-details/marriott-international-update-conclusion-uk-ico-investigation

8 The Markup. Blacklight: A real-time website privacy inspector. https://themarkup.org/blacklight

9 Google. PageSpeed Insights. https://pagespeed.web.dev

Қорғау шаралары

10 Cybersecurity and Infrastructure Security Agency (CISA). (2022, October). Implementing phishing-resistant MFA [Fact sheet]. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

11 MGM Resorts International. (2023, October 5). Form 8-K. U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

12 Federal Bureau of Investigation, IC3. (2022, January 18). Cybercriminals tampering with QR codes to steal victim funds. https://www.ic3.gov/PSA/2022/PSA220118

13 Federal Bureau of Investigation, IC3. (2022, February 8). Criminals increasing SIM swap schemes to steal millions of dollars from US public. https://www.ic3.gov/PSA/2022