INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-13 16:28 UTC

Booking.com Breach Exposes Reservation PII, Enables Targeted Phishing Campaigns

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0089
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Booking.com online travel platform (accommodation, flights, car rentals, travel experiences), all affected reservation holders
Published	2026-04-13T13:30:10
Discovery Source	Rss

Executive Summary

Booking.com confirmed unauthorized access to guest reservation data, exposing full names, email addresses, phone numbers, postal addresses, and booking details for an undisclosed number of affected travelers. Threat actors are actively weaponizing this reservation-level data, including trip dates, destinations, and confirmation numbers, to run highly targeted phishing campaigns against affected customers. Organizations whose employees book business travel through Booking.com face immediate credential theft and fraud risk from convincing impersonation attacks.

Technical Analysis

This is a data breach incident, not a software vulnerability, no CVE has been assigned. The exposure maps to CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) and CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor). Compromised data includes PII and reservation-specific details sufficient for contextually accurate social engineering. MITRE ATT&CK techniques in active or probable use include T1589.002 (Gather Victim Identity Information: Email Addresses), T1598.003 (Phishing for Information: Spearphishing Link), T1566.002 (Phishing: Spearphishing Link), T1586.002 (Compromise Accounts: Email Accounts), T1534 (Internal Spearphishing), and T1659 (Content Injection). T1078 (Valid Accounts) is relevant if phishing yields credential compromise. Booking.com has forced PIN resets on affected reservations and issued breach notifications, but has not disclosed victim count or the initial access vector. No patch is applicable, this is a provider-side breach with no customer-deployable fix. Qualitative severity rating of High reflects large-scale PII exposure enabling downstream fraud; CVSS and EPSS (Exploit Prediction Scoring System) apply only to software vulnerabilities with known exploits, not to breach incidents, therefore are not applicable here.

Action Checklist

1. Response & Communication: Alert employees and customers who may have booked travel via Booking.com accounts linked to corporate email addresses. Instruct them not to click links in any reservation-related emails until the phishing campaign scope is confirmed. Flag Booking.com notification emails as high-risk vectors requiring manual verification.
2. Detection: Monitor email security gateways and SIEM for inbound messages referencing Booking.com reservation language, confirmation numbers, or travel itinerary details. Look for lookalike sender domains (e.g., booking-confirmation[.]com, reservations-bookingcom[.]net). Query mail logs for emails containing booking confirmation number patterns paired with external links delivered to employees in the affected window (post-April 13, 2026).
3. Eradication: There is no customer-side patch. Eradication depends on Booking.com's remediation of the initial access vector, which has not been disclosed. For internal exposure: rotate credentials for any corporate accounts where Booking.com email addresses overlap with SSO or Active Directory credentials. Revoke and re-issue any API keys or tokens used for corporate travel booking integrations with Booking.com.
4. Recovery: Validate that affected employee accounts show no unauthorized access via identity provider logs. Confirm no lateral movement from compromised credentials by reviewing authentication events in your IdP (e.g., Okta, Azure AD, Entra ID) for anomalous login patterns post-April 13, 2026. Restore normal email trust settings only after your email security platform has updated phishing signatures covering this campaign.
5. Post-Incident: Assess whether corporate travel booking workflows create downstream credential risk by reusing email addresses across SaaS platforms. Implement phishing-resistant MFA (FIDO2/passkeys) for accounts linked to high-value travel booking personas. Review third-party travel vendor security requirements in vendor risk management program; add breach notification SLA requirements to Booking.com and similar travel platform contracts.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if any blast-radius employee account shows confirmed unauthorized IdP authentication post-April 13, 2026, if the organization operates in a jurisdiction requiring breach notification for employee PII exposure (e.g., GDPR Article 33, CCPA), or if Booking.com travel integration API keys are confirmed to have accessed internal systems — any of these conditions triggers regulatory notification timelines and potential liability.

Recovery Notes	Recovery is gated on two external dependencies neither of which the organization controls: Booking.com's disclosure of the initial access vector and remediation timeline, and email security vendor signature updates covering the active phishing campaign using stolen reservation PII. Monitor IdP authentication logs for the blast-radius account list for a minimum of 30 days post-credential-rotation, as threat actors holding reservation-level PII (including trip dates and confirmation numbers) may time follow-on phishing attempts to coincide with actual travel dates visible in the stolen booking data. Maintain elevated email gateway scrutiny rules for all reservation-themed inbound mail until Booking.com publicly confirms the unauthorized access has been fully remediated.
Forensic Artifacts	Email gateway message trace logs (Microsoft 365 Get-MessageTrace / Google Workspace Admin Email Log Search) for inbound messages from April 13, 2026 onward containing Booking.com reservation language, confirmation number patterns, or lookalike sender domains — these are the primary evidence of active phishing campaign delivery against your organization | IdP authentication logs (Okta System Log event types user.session.start and user.authentication.sso; Azure AD / Entra ID Sign-in logs including riskLevelDuringSignIn field) scoped to blast-radius accounts from April 13, 2026 onward — anomalous entries here indicate credential compromise resulting from employees engaging with reservation-themed phishing emails | Active Directory or Entra ID account attribute exports (LastLogonDate, PasswordLastSet, BadPwdCount) for blast-radius accounts captured before credential rotation — establishes pre-incident baseline and may reveal accounts already accessed by threat actors using credentials harvested via the Booking.com breach-enabled phishing campaign | Corporate travel booking integration API gateway access logs and token last-used timestamps for any Booking.com Connectivity Partner API keys or OAuth tokens — confirms whether integration credentials were exposed in the breach dataset and whether they have been used for unauthorized API calls against internal travel management or expense systems | Browser history and endpoint DNS cache artifacts (Windows: ipconfig /displaydns; macOS: sudo dscacheutil -cachedump; Chrome History SQLite DB at %LOCALAPPDATA%\Google\Chrome\User Data\Default\History) from devices belonging to blast-radius employees who reported clicking reservation-themed email links — identifies the specific lookalike phishing domains and landing pages used in this campaign

Per-Action IR Details

Containment — Alert employees and customers who may have booked travel via Booking.com accounts linked to corporate email addresses. Instruct them not to click links in any reservation-related emails until the phishing campaign scope is confirmed. Flag Booking.com notification emails as high-risk vectors requiring manual verification.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected communication channels and limit further exposure from active phishing campaigns weaponizing stolen Booking.com reservation PII

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST SI-3 (Malicious Code Protection), CIS 9.6 (Block Unnecessary File Types) — block or quarantine inbound emails matching Booking.com reservation language patterns at the gateway, CIS 17.4 (Establish and Maintain an Incident Response Process)

Compensating: For teams without enterprise email security: deploy a mail transport rule in Microsoft 365 (via Exchange Admin Center > Mail Flow > Rules) to prepend a warning banner to any inbound email where the sender domain does not exactly match booking.com but contains the string 'booking' or 'reservation'. Export the rule via PowerShell: Get-TransportRule | Export-Clixml rules_backup.xml. For Google Workspace, use Compliance > Content Compliance rules with similar string matching. Distribute a one-paragraph user advisory over a trusted internal channel (Slack, Teams, or intranet) explicitly naming the threat: stolen Booking.com reservation data including confirmation numbers and trip dates is being used to craft convincing phishing emails — treat all reservation-related emails as

suspect regardless of apparent sender.

Evidence: BEFORE issuing the alert, capture a snapshot of your email gateway quarantine queue and inbound mail logs for the window April 13, 2026 to present, filtered on sender domains containing 'booking', 'reservation', or 'itinerary'. Preserve raw message headers (SMTP envelope, Received chain, DKIM/SPF/DMARC authentication results) for any suspicious reservation-themed emails already delivered. Document the list of corporate email addresses confirmed as Booking.com account holders — this is the definitive blast radius list for all downstream steps.

Detection — Monitor email security gateways and SIEM for inbound messages referencing Booking.com reservation language, confirmation numbers, or travel itinerary details. Look for lookalike sender domains (e.g., booking-confirmation[.]com, reservations-bookingcom[.]net). Query mail logs for emails containing booking confirmation number patterns paired with external links delivered to employees in the affected window (post-April 13, 2026).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate email gateway telemetry, IdP authentication events, and endpoint process logs to identify employees who received and potentially interacted with phishing emails constructed from stolen Booking.com reservation PII

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 9.7 (Deploy and Maintain Email Server Anti-Malware Protections)

Compensating: Without a SIEM, perform the following manual queries: (1) Microsoft 365: use the Security & Compliance Center > Content Search or Exchange Online PowerShell — Search-Mailbox or Get-MessageTrace — filtering RecipientAddress to the blast-radius employee list, SenderAddress NOT EQUAL to *@booking.com, and subject/body containing terms like 'reservation', 'confirmation', 'itinerary', 'check-in'. Export results to CSV. (2) For lookalike domain detection without a threat intel feed, query your DNS resolver logs or firewall outbound DNS logs for any resolution of domains matching regex booking[\-\.].*\.(com|net|org) excluding exact booking.com. Use grep on exported logs: grep -P 'booking[-\.][^.]+\.(com|net)' dns_query.log. (3) Deploy the free Sigma rule 'Phishing Email with Lookalike Domain' (SigmaHQ GitHub, rules/email category) converted to your log format using sigma-cli.

Evidence: Export Microsoft 365 Unified Audit Log or Google Workspace Admin Audit for MailItemsAccessed and Send events scoped to the blast-radius employee list from April 13, 2026 onward — this identifies both received phishing emails and any account compromise enabling inbox access by a third party. Collect SMTP message trace logs showing full delivery path, sender IP, and authentication headers for all reservation-themed messages. If any employee clicked a link, retrieve browser history or endpoint DNS cache (ipconfig /displaydns on Windows, sudo dscacheutil -cachedump on macOS) to identify the destination URL. Preserve all artifacts before issuing any remediation instructions that could trigger log rotation or cache clearing.

Eradication — There is no customer-side patch. Eradication depends on Booking.com's remediation of the initial access vector, which has not been disclosed. For internal exposure: rotate credentials for any corporate accounts where Booking.com email addresses overlap with SSO or Active Directory credentials. Revoke and re-issue any API keys or tokens used for corporate travel booking integrations with Booking.com.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove threat actor footholds by eliminating credential overlap between the breached Booking.com platform and internal identity infrastructure, and revoking all integration tokens that may have been exposed in the breach dataset

Controls: NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation), NIST CM-8 (System Component Inventory), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without PAM tooling: (1) Use Active Directory PowerShell to force a password reset for all accounts whose UPN or associated email matches the Booking.com blast-radius list: Get-ADUser -Filter {EmailAddress -like '*@yourdomain.com'} -Properties EmailAddress | Set-ADUser -ChangePasswordAtLogon $true. Scope this to the confirmed blast-radius list only, not a blanket reset, to avoid operational disruption. (2) For API key/token revocation: query your API gateway access logs or secret manager (HashiCorp Vault audit log, AWS IAM last-used report, or a

manual registry of integration credentials) for any tokens scoped to Booking.com travel integrations. Revoke immediately via the Booking.com Connectivity Partner portal or your travel management platform's admin console. Document each revoked credential with timestamp for the post-incident record. (3) Check for credential reuse using the free haveibeenpwned API (haveibeenpwned.com/API/v3) against the blast-radius email list to identify accounts with prior breach exposure compounding the current risk.

Evidence: Before rotating credentials, capture a read-only export of current Active Directory account attributes (LastLogonDate, PasswordLastSet, BadPwdCount) for all blast-radius accounts using Get-ADUser with -Properties * piped to Export-Csv — this establishes a pre-rotation baseline to compare against post-incident. Export the Booking.com Connectivity Partner API key inventory and last-used timestamps if accessible. Preserve IdP session token logs (Okta System Log: event type user.session.start; Azure AD Sign-in logs) for the blast-radius accounts for the April 13, 2026 onward window before any session invalidation, as these may show unauthorized access that already occurred using exposed credentials.

Recovery — Validate that affected employee accounts show no unauthorized access via identity provider logs. Confirm no lateral movement from compromised credentials by reviewing authentication events in your IdP (e.g., Okta, Azure AD, Entra ID) for anomalous login patterns post-April 13, 2026. Restore normal email trust settings only after your email security platform has updated phishing signatures covering this campaign.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verify integrity of identity infrastructure and email trust posture before returning affected accounts and communication channels to normal operational status following credential rotation and token revocation

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-2 (Account Management), NIST SI-4 (System Monitoring), CIS 6.1 (Establish an Access Granting Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 8.2 (Collect Audit Logs)

Compensating: Without a commercial IdP UEBA module: (1) In Okta, run a System Log export filtered on event types user.session.start, user.authentication.sso, and policy.evaluate_sign_on for the blast-radius account list post-April 13, 2026. Flag any login events from IP addresses not previously associated with the user (new ASN, new country, or impossible travel — two authentications from geographically distant IPs within a timeframe that precludes physical travel). Export via Okta API: GET /api/v1/logs?filter=eventType+eq+%22user.session.start%22&since=2026-04-13T00:00:00Z. (2) In Azure AD / Entra ID, use the Risky Sign-ins report (Identity Protection blade) or PowerShell: Get-AzureADAuditSignInLogs -Filter "createdDateTime ge 2026-04-13" | Where-Object {$_.riskLevelDuringSignIn -ne 'none'}. (3) Do not lift elevated email scrutiny rules until your email security vendor (Proofpoint, Mimecast, Defender for Office 365, or equivalent) confirms updated detection signatures for this specific Booking.com phishing campaign — check vendor threat intelligence bulletins explicitly.

Evidence: Before restoring normal email trust settings, collect a final snapshot of the email gateway quarantine queue to confirm no new lookalike-domain reservation phishing emails arrived post-credential-rotation — new arrivals after rotation suggest the phishing campaign is continuing independently of credential compromise and the containment rule must remain active. Preserve the full IdP authentication log export for the blast-radius accounts covering April 13, 2026 through recovery completion as the authoritative record for any regulatory breach notification or insurance claim. Document the specific signature version or rule update from your email security platform that covers this campaign before marking recovery complete.

Post-Incident — Assess whether corporate travel booking workflows create downstream credential risk by reusing email addresses across SaaS platforms. Implement phishing-resistant MFA (FIDO2/passkeys) for accounts linked to high-value travel booking personas. Review third-party travel vendor security requirements in vendor risk management program; add breach notification SLA requirements to Booking.com and similar travel platform contracts.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review to address the structural risk that corporate email address reuse across consumer travel platforms creates a persistent, vendor-dependent exposure surface that exceeds the organization's direct control

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services), NIST IA-5 (Authenticator Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 15.1 (Establish and Maintain an Inventory of Service Providers)

Compensating: Without a formal vendor risk management platform: (1) Build a simple spreadsheet inventory of all SaaS travel platforms (Booking.com, Expedia, Concur, TripActions, Navan) where corporate email addresses are registered, noting whether each platform supports FIDO2/passkey MFA — this directly addresses the credential-reuse exposure this breach demonstrated. (2) For FIDO2 rollout without a commercial identity platform: Microsoft Entra ID Free tier supports FIDO2 security keys (YubiKey, Google Titan) for MFA — enable via Azure AD > Authentication Methods > FIDO2 Security Key policy, scoped initially to the travel-booking blast-radius group. (3) Draft a one-page vendor security addendum covering mandatory breach notification within 72 hours, annual SOC 2 Type II report sharing, and incident communication SLAs; attach to renewal negotiations with Booking.com's corporate/business travel program. Reference NIST SP 800-161 (Supply Chain Risk Management) as the methodology basis for the vendor addendum.

Evidence: For the lessons-learned record, document the precise timeline from Booking.com's breach date to your organization's first detection of phishing attempts targeting employees — this gap measurement is the primary metric for evaluating the adequacy of your current third-party breach monitoring capability (e.g., whether you subscribe to HaveIBeenPwned Enterprise, FS-ISAC, or a commercial threat intelligence feed that would have surfaced this breach earlier). Retain all IR artifacts — blast-radius account list, email gateway rule change history, credential rotation log, IdP authentication exports — for a minimum of one year to support any regulatory inquiry under applicable data protection obligations triggered by employee PII exposure.

Detection Guidance

No IOCs from this breach have been publicly confirmed as of the item date (2026-04-13). Detection should focus on behavioral and contextual indicators. In email security platforms (Proofpoint, Mimecast, Microsoft Defender for Office 365): create rules flagging inbound messages containing Booking.com branding, reservation confirmation language, or itinerary details combined with external links or attachment payloads. In SIEM, query for authentication events from employees who received Booking.com-themed emails in the 48-72 hours following receipt. Monitor for newly registered domains containing 'booking', 'reservation', or 'travel' variants (passive DNS feeds, DomainTools, or similar). Watch for T1598.003 indicators: unexpected credential harvest pages mimicking Booking.com login flows appearing in proxy or DNS logs. If employees report unexpected PIN reset emails from Booking.com, treat these as potentially leveraged for pretexting rather than confirming breach remediation.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not confirmed as of 2026-04-13`	No specific phishing domains or infrastructure have been publicly attributed to this campaign in available sources. Monitor for lookalike Booking.com domains via passive DNS and threat intelligence feeds.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1534** — Internal Spearphishing
- **T1586.002** — Email Accounts
- **T1659** — Content Injection
- **T1589.002** — Email Addresses
- **T1598.003** — Spearphishing Link
- **T1586** — Compromise Accounts
- **T1566.002** — Spearphishing Link
- **T1598** — Phishing for Information

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1534	Internal Spearphishing	Lateral-Movement
T1586.002	Email Accounts	Resource-Development
T1659	Content Injection	Initial-Access
T1589.002	Email Addresses	Reconnaissance
T1598.003	Spearphishing Link	Reconnaissance
T1586	Compromise Accounts	Resource-Development
T1566.002	Spearphishing Link	Initial-Access
T1598	Phishing for Information	Reconnaissance

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-bookingcom-data-...	T3
Booking.com warns customers of hack that exposed their data	https://www.theguardian.com/technology/2026/apr/13/booking-com-cust...	T2
Double-Check Your Travel Reservations. Booking.com Hit by Data ...	https://uk.pcmag.com/security/164382/double-check-your-travel-reser...	T3
Huge data breach as major travel site is hacked - Daily Mail	https://www.dailymail.co.uk/news/article-15728033/Booking-data-brea...	T3

Source	URL	Tier
Booking.com have had a few data breaches so be aware when ...	https://www.facebook.com/groups/596526160767608/posts/2322820901471...	T3

Generated 2026-04-13 16:28 UTC by TJS Security Command Center