The Impact of ClickFix Attacks on Booking.com

Sayed Edris Sadeed

Ben Reino

Nabila Nawsheen

Pedro Raji

Shawn Douglas

October 2025

George Brown College

Cyber Security (Postgraduate) - T433

Abstract

Cybersecurity attacks are becoming increasingly sophisticated, and ClickFix malware has emerged as a major threat. Since its first identification in late 2024, ClickFix attacks have escalated rapidly, with 47% of reported incidents occurring in March 2025 alone (An, 2025). Booking.com, as a leading e-commerce and hospitality platform, is a high-value target due to its extensive stores of sensitive customer information.

ClickFix primarily targets confidentiality by exploiting human vulnerabilities. The breach typically begins with a phishing email disguised as an official Booking.com request. When a recipient clicks the link or opens the malicious attachment, they are shown a pop-up requesting their action to 'fix' a computer issue by following three simple steps. The first step requests the user to press the windows key and the R key together. This opens the run function. The second step asks the user to press Ctrl and V, which pastes the malware into the run window. The malware script is preloaded onto the site's virtual clipboard, allowing it to be copied and pasted, unbeknownst to the user (McGowan, 2025). The third and final step simply asks the user to press enter, which executes the malware (Krebs, 2025). Once the malware installs itself, it captures login credentials and other sensitive data through infostealers such as AsyncRAT, Danabot, DarkGate, Lumma Stealer, NetSupport, and more (Madjar, 2024). This information is then transmitted to the attacker's servers, enabling unauthorized access to employee credentials that can grant access to the hotel's computers. This unauthorized access led to the theft of customer accounts, names, reservation numbers and travel history. With this information, threat actors then send fraudulent emails, WhatsApp or SMS messages to guests, using their names, reservation numbers and dates of travel, giving the messages an appearance of authenticity, asking to confirm their banking details or offering attractively priced upgrades. This completes the attack chain when the guests unwittingly give the threat actors their banking information (Scion, 2025).

Using the McCumber Cube framework (McCumber, 2004), this study analyzes the impact of ClickFix attacks on information security across three states: storage, transmission, and processing, and across three protection layers: policy, ETA, and technology. By examining how ClickFix exploits weaknesses at each intersection, the study provides practical recommendations for strengthening Booking.com's cybersecurity and safeguarding the confidentiality, integrity, and availability of customer information.

Confidentiality × Storage × Policy/Procedures

When attackers obtain access to the internal networks of the hotel using ClickFix attacks, through the malware that is inadvertently downloaded by hotel staff, they can exfiltrate data at rest. This data includes personal guest information, such as their name, reservation numbers, name of the hotel they will stay at and the dates of travel. Confidentiality is severely compromised as soon as unauthorized users obtain sensitive information at rest. Policy controls can greatly mitigate this form of attack. A policy stating that no staff, under any circumstances, are to perform fixes of any kind. Any fixes are to be first observed and handled by the IT department. This policy will have to be coupled with further training and education which is detailed below. There must be frequent auditing to confirm that sensitive information is encrypted and stored in safe locations. Role-based access control (RBAC) can be employed to restrict data access to sensitive information for privileged employees who need access to it for legitimate business purposes.

Confidentiality × Storage × Education Training and Awareness

Human factors and their awareness, or lack thereof, play the biggest role in ClickFix attacks. Users (the majority of whom are hotel staff) are lured into executing harmful code that grants attackers access to stored sensitive data. Phishing messages that impersonate Booking.com will engage the user by requesting their immediate attention to a matter. For example, a staff member of a hotel that uses the Booking.com platform, received an email seemingly from Booking.com about an unhappy guest leaving a bad review and a reply must be given in 24 hours. The email asks the recipient to click a link that will allow them to reply to the review. Once the link has been clicked, the recipient is then shown a pop-up where they are requested to perform the three steps detailed in the abstract above. This introduces the malware to the hotel's network. Without human action, the malware would never be introduced. Regular training on what to look for should be made obligatory for all employees. This should involve emphasizing the dangers of phishing mail and other social engineering techniques, as well as showing employees examples of what the phishing emails look like as well as the fake pop-ups that get employees to paste and execute the malware. Conducting mock phishing attacks to test employees' vigilance and ensuring they can identify potential threats should be implemented. One further recommendation is to educate the guests that use Booking.com to book their hotels. A banner can be added to the page once they have confirmed their reservation noting that Booking.com or the hotel they will be visiting will NEVER contact them asking for further information. If they do receive communication asking for further information, disregard and send the email to the Booking.com Cybersecurity team.

Confidentiality × Storage × Technology

While ClickFix attacks rely on social engineering to introduce malware, and there is no evidence of technological failures that allow these attacks to succeed, there are technological controls that can used to mitigate ClickFix attacks. To protect stored data, encryption should be enforced at the file level, and antivirus software should be updated constantly so that it can recognize and prevent malicious files. Advanced endpoint defense (such as EPP or EDR) can detect and isolate suspicious activity on users' computers. Lastly, a simple yet effective control would be activating group policy restrictions, disabling the use of the Windows key + R opening the run feature, therefore stopping Step 1 of the attack before any malware can even be pasted and then executed (Krebs, 2025).

Confidentiality × Transmission/Processing × Policy/Procedures

Throughout the research done for this report, no evidence was found that data in transmission or in process was ever compromised. ClickFix attacks at this point have attacked data in storage. As such, the confidentiality of data in transmission and in process will be discussed together. As outlined in the abstract, Remote Access Trojans (RATs) have been discovered as malware introduced through ClickFix attacks (An, 2025). Due to the existence of RATs, which give attackers wide access over the compromised networks, there is a potential for future data breaches when data is transmitted on insecure channels can be intercepted or modified and hence produce a data leak. Since attackers can intercept such transmission channels, they can steal or divert information intended for lawful

recipients. All confidential data transmitted through email, SMS, or any other mode of communication must be encrypted using TLS/SSL. Booking.com must also implement email filtering mechanisms that can prevent phishing emails and prevent malicious attachments from reaching employees. Secure transmission protocols must be implemented to ensure confidentiality of in-transit data.

Confidentiality × Transmission/Processing × Education Training and Awareness

The root cause of confidentiality breaches in data transmission is human error. Employees, for example, may inadvertently open a malicious attachment or be socially engineered and leak sensitive information during transmission. Again, this is not shown by evidence. These are potential scenarios and proactive recommendations based on the information gathered about ClickFix attacks. Employees unintentionally pass on customer sensitive information by insecure channels or disclose it to unauthorized parties. This kind of human error might cause data to be intercepted in transit without permission, violating customer privacy. Staff awareness training is the most important step to reduce human error. Staff needs to be educated on secure ways of communicating, i.e., not sending sensitive information through insecure channels. Also, technologies such as email encryption or secure file transfer mechanisms should be adopted to prevent accidental information leakage.

Confidentiality × Transmission/Processing × Technology

Technical weaknesses in the encryption of transmission channels can allow attackers to intercept or redirect sensitive information in transit. It is important to note that at this time, there is no evidence that data in transmission or in process has been compromised. If ClickFix malware spreads through the network, it can potentially intercept insecure communications and obtain sensitive information. Without adequate technical countermeasures, transmission channels will be vulnerabilities through which attackers can intercept or alter sensitive information and lead to severe compromises of confidentiality. These suggested controls are a proactive measure to mitigate the potential of intercepting data in transmission. Robust encryption methods (such as VPN or end-to-end encryption) must be implemented on all communication channels to secure data in transit. Safe communication channels such as HTTPS and SFTP need to be employed while transmitting sensitive customer data to ensure the integrity and confidentiality of data being transmitted.

Integrity

Integrity ensures that data remains accurate, consistent, and protected from unauthorized modification. In the context of the ClickFix malware campaign, data integrity at Booking.com is at risk due to unauthorized data manipulation, malware-driven script execution, and credential abuse after employees unknowingly execute malicious commands (Microsoft, 2025; Krebs, 2025). Attackers can modify booking information, change reservation availability, alter financial transactions, and corrupt configuration files, severely impacting data trust and system reliability (Proofpoint, 2025).

When Data is in Process

During live booking operations or payment authorization, ClickFix can interfere with transaction integrity by modifying values in real time. Attackers can inject malicious scripts that manipulate reservation quantities, apply unauthorized discounts, alter partner payout values, or duplicate

transactions during active processing (Proofpoint, 2025). These silent changes corrupt live data streams before they are committed to storage, resulting in false confirmations or financial miscalculations. Because ClickFix exploits legitimate browser sessions, compromised employees unknowingly process tampered data through PMS dashboards and Booking.com's internal tools (Microsoft, 2025).

Education, Training, and Awareness
Employees need integrity-focused training to identify suspicious script pop-ups, unauthorized transaction changes, and abnormal clipboard behavior during booking operations. Continuous phishing simulations teaching staff to block malicious automation attempts help mitigate human-enabled integrity loss (Cofense, 2025).

Policy
Transaction integrity policies should enforce dual approval for high-risk changes, automated verification for booking modifications, and audit controls for financial transactions to prevent unauthorized tampering (Whitman & Mattord, 2022).

Technology
Implementing Runtime Application Self-Protection (RASP), API validation gateways, and transaction integrity monitoring can detect unauthorized payload modifications during processing. Real-time script filtering and anti-code injection tools must be deployed across booking workflows (IBM Security, 2024).

When Data is Stored
Once attackers gain persistence through ClickFix, they may alter stored booking inventories, customer profiles, partner commission rates, and refund rules within internal databases (Cofense, 2025). Tampering with stored data enables fraud such as false refunds, phantom reservations, or manipulated payout balances. Silent manipulation of stored configuration files can also introduce long-term business logic corruption, making transactional data unreliable over time (Whitman & Mattord, 2022).

Education, Training, and Awareness
Human error can also affect data integrity when employees unintentionally overwrite or modify stored data after following malicious ClickFix instructions. Training staff to verify unusual configuration changes and report abnormal database edits prevents unnoticed tampering.

Policy
Strong data governance policies must enforce role-based access control (RBAC), change approval workflows, and tamper-evident logging for all stored booking data. Integrity validation policies should require regular reconciliation between core records and partner systems.

Technology
To prevent stored data manipulation, Booking.com should deploy File Integrity Monitoring (FIM), Database Integrity Monitoring (DIM), and cryptographic validation (checksums, hashing) across

critical data repositories. Tools such as Tripwire and CrowdStrike Falcon can detect unauthorized modifications (IBM Security, 2024).

When Data is in Transmission

Booking.com relies on constant data exchange between partner PMS systems, internal microservices, and third-party APIs. ClickFix threatens data integrity in transit by stealing session cookies and API tokens to alter booking payloads mid-transmission (Microsoft, 2025). Attackers can intercept reservation updates, change stay dates, edit amounts, or manipulate payment confirmations before they reach Booking.com servers. This causes system mismatches, financial disputes, and reconciliation failures between partners and Booking.com (Cofense, 2025).

Education, Training, and Awareness

Without training, employees may unintentionally forward sensitively booking data over insecure channels or accept fraudulent API messages, allowing attackers to tamper with transmitted data.

Policy

Policies must mandate encrypted channels (TLS 1.2+), API authentication rotation, certificate pinning, and integrity verification for every booking update. Replay protection and message authenticity rules are critical for safeguarding transmission integrity (Whitman & Mattord, 2022).

Technology

Integrity of transmitted data can be maintained through Hash-based Message Authentication Codes (HMAC), digital signatures, and API anomaly detection systems. Gateway-level data validation must ensure no tampering occurs during transit.

Availability

ClickFix can quickly degrade Booking.com's availability through credential theft, API abuse, and destructive payloads. Attackers can compromise systems, alter reservations, misuse API keys, or deploy malware that disrupts essential services, potentially blocking guest bookings and causing operational downtime. In a real incident, a critical Booking.com API outage reported via ClickFix caused reservation data to stop syncing with hotel systems, preventing staff from accessing upcoming bookings (KrebsOnSecurity, 2025). This led to double bookings, missed reservations, and temporarily unavailable historical data, directly impacting hotel operations and guest experience, showing how potential attack scenarios can translate into real-world disruptions (Malwarebytes, 2025).

When Data is in Process:

The investigation shows that live operational processes were affected when staff were tricked into executing commands that installed malware, resulting in compromised credentials. Microsoft details this attack flow and the immediate compromise of partner accounts (Microsoft, 2025). Once control was gained, attackers sent messages and performed reservation related actions through the hotel's live processing channels. KrebsOnSecurity confirms that attackers used these hijacked accounts to contact customers, showing abuse of in-process operations (KrebsOnSecurity, 2025).

It is inferred that temporary suspension of automated messaging or manual verification of high-risk transactions would be required to prevent further misuse. This reduces the performance of live processing, although not explicitly stated in the sources. Malwarebytes documents that the RATs delivered via fake Booking.com pages helped execute the attack, outlining the risk to in-process data (Malwarebytes, 2025). Containment measures, inferred from standard incident-response best practices (NIST SP 800-61 Rev. 2, Page 41, Section 3.3.1), are necessary to restore trusted operation which would reduce availability until live processing systems are verified to be safe.

When Data is Stored:

Once attackers authenticated the partner's account, they obtained access to stored reservation records and account settings, making those records operationally untrusted. KrebsOnSecurity confirms that compromised accounts were used to send unauthorized messages to guests, demonstrating exposure of stored data (KrebsOnSecurity, 2025).

Malwarebytes reports that fake Booking.com pages and redirected links delivered RATs facilitating credential theft and data exfiltration (Malwarebytes, 2025). It is inferred that limiting access or isolating compromised accounts would have been necessary to maintain control over stored data. Attackers could export or modify reservation data, requiring verification, forensic analysis, and credential resets before data could be trusted again. These steps logically extend the downtime and make stored reservation data temporarily unavailable until validated restoration and verification procedures are completed.

Education, Training and Awareness:

Staff must receive scenario-based training on credential hygiene, secure endpoint use, and proper extranet access, including avoiding execution of Windows Run copy and paste instructions from phishing pages like ClickFix. Phishing simulations using Booking.com themed lures paired with exercises can reinforce staff members' ability to recognize malicious prompts and escalation procedures. These exercises prepare personnel to maintain availability of stored reservation data and live processing channels by quickly isolating compromised accounts and switching to manual operations when necessary.

Policy:

As part of mitigating the breach, all partner and extranet accounts must use multi-factor authentication and enterprise credential vaults to prevent the theft of credentials. Administrative access must be restricted to dedicated, hardened workstations with least-privilege roles to separate critical systems from general endpoints. Backups of reservation data should be kept in a way that they cannot be changed or deleted, and each backup should be checked with a digital fingerprint to make sure the data is exactly the same as when it was created to allow for rapid restoration.

Messaging and live reservation data should be monitored via filtered gateways with anomaly detection and throttling to prevent abuse, preserving in-process availability.

Technology:

The attack leverages endpoint vulnerabilities, stolen credentials, and partner APIs. While Booking.com's core stored data remains secure, attackers can disrupt synchronization, flood APIs, or halt services via RATs or malware, making listings and reservations temporarily unavailable. Proper EDR, network segmentation, and backup integrity are critical to maintaining availability.

Data in Transmission:

Booking.com constantly exchanges reservation data, customer details, payment confirmations, and availability updates across its cloud infrastructure and partner APIs. Property Management Systems (PMS), channel managers, OTAs, and payment processors all push and pull booking and inventory data, creating two main transit layers: internal cloud-to-cloud communication and external partner API traffic, being the most exposed to ClickFix-driven compromise(Booking.com API / Connectivity).

If ClickFix infects a partner system and steals API keys or tokens, attackers could intercept, modify, or disrupt API requests, causing inconsistent or unavailable data during transmission. A compromised PMS endpoint can break synchronization processes or corrupt local booking caches, leading to delayed or failed reservation updates.

While there is no public evidence that ClickFix campaigns have directly slowed or blocked Booking.com API traffic, the malware's credential-theft and endpoint-disruption capabilities make such interference plausible. Booking.com has already experienced API outages where reservation data stopped syncing, demonstrating how similar failures could occur if ClickFix affects the same transmission channels.

Education, Training, and Awareness

Users or staff can unintentionally expose data in transit by following ClickFix-style instructions that trick them into running commands or sharing credentials over insecure channels. Poor awareness of phishing and secure communication practices increases the chance that attackers obtain tokens used for live API sessions, which can lead to disrupted booking-data sync. While there is no evidence of ClickFix directly causing API transmission failures, human error remains a pathway that could enable the same type of sync disruption Booking.com has already experienced during API outages.

Policy

Weak policy enforcement such as inconsistent TLS requirements, lax authentication rules, or long-lived tokens can worsen the impact of a ClickFix compromise by making intercepted credentials more usable. Strong policies around encrypted communication, short token lifetimes, continuous API monitoring, and rapid incident response help preserve data availability even if attackers attempt to interfere with transmission. These measures reduce the likelihood that a ClickFix-enabled breach could trigger the kind of booking-sync failures seen during past Booking.com API disruptions.

Technology

ClickFix can compromise partner or endpoint systems to harvest credentials or session tokens, giving attackers the ability to interfere with API calls between PMS systems, partners, and Booking.com servers.

Encryption protects the data itself, but once an endpoint is compromised, attackers can still disrupt or delay transmissions. Although ClickFix has not been shown to directly block Booking.com's APIs, the malware's capabilities make such interference plausible, especially given that Booking.com has already experienced API outages where reservation data temporarily stopped syncing, showing how availability could be similarly affected.

References

1.Arntz, Pieter (2025, June 2)

https://www.malwarebytes.com/blog/news/2025/06/victims-risk-asyncrat-infection-after-being-redirected-to-fake-booking-sites

2.Erman, B. (2025, October 14)
https://www.terranovasecurity.com/blog/clickfix-scams-how-cybercriminals-exploit

3.HHS / HC3 Sector Alert - 'ClickFix Attacks' - broader context on ClickFix attacks across sectors, including hospitality (October 2024).

4.Infosecurity Magazine - ClickFix Phishing Scam Targets Hospitality (2025).

5.Kahng, A. (2025, June 4)

https://cofense.com/blog/clickfix-campaign-spoofs-booking-com-for-malware-delivery

6.Krebs, B. (2025, March 14)
https://krebsonsecurity.com/2025/03/clickfix-how-to-infect-your-pc-in-three-easy-steps/

7.Madjar, T. (November 18, 2024)
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape

8.Mascellino, A. (2025)
Phishing Campaign Uses Fake Booking.com Emails to Deliver Malware

9.McCartney, A. (2024, April 3)

https://infosectaskforce.com/index.php/2024/04/03/the-mccumber-cube-model

10.McCumber, J. (2004, June 15)

https://everything.explained.today/McCumber_cube/

11.McGown, E. (2025, March 26)

https://cyberresilience.com/threatonomics/understanding-the-clickfix-attack/

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

13.Mline (2011, December 10)

https://nedatanet.com/certification/mgmt-info-sec-notes-week1

14.Partner.booking.com (2025, February) https://partner.booking.com/en-us/help/legal-security/security/online-security-awareness-phishing-and-email-spoofing

15.Proofpoint. (2025). *Security Brief: ClickFix social engineering attacks*.

16.Ramdas, A. (2025, June 2)

https://medium.com/%40anjuramdas15/the-mccumber-cube-a-timeless-framework-for-information-security-6af276999421

17.Saraswati, N. (2021, February 21)

https://medium.com/it-paragon/the-cybersecurity-cube-cff88638d8e7

18.Scion, Jeremey (2025, November 6)

https://blog.sekoia.io/phishing-campaigns-i-paid-twice-targeting-booking-com-hotels-and-customers/

19.St. John, C. (2024, November 22)

https://medium.com/%40csjcode/cia-triad-in-cloud-security-part-1-confidentiality-b7ec5dcf21a2

20.Whitman, M. & Mattord, H. (2022). *Management of Information Security* (7th Ed.).

21.Yadav, C. (2023, March 30)

https://medium.com/%40cjyadav/cybersecurity-cube-of-an-organization-b07d92e31992

22. Microsoft Security Blog. (2025). *ClickFix attack campaign analysis*

23. Cofense. (2025). *Phishing trends in the hospitality sector*