Partners Universal International Research Journal (PUIRJ)
Volume: 03 Issue: 04 | October – December 2024 | ISSN: 2583-5602 | www.puirj.com

Personal Privacy at Risk: The Security Threats of Sharing Boarding Passes Online

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India

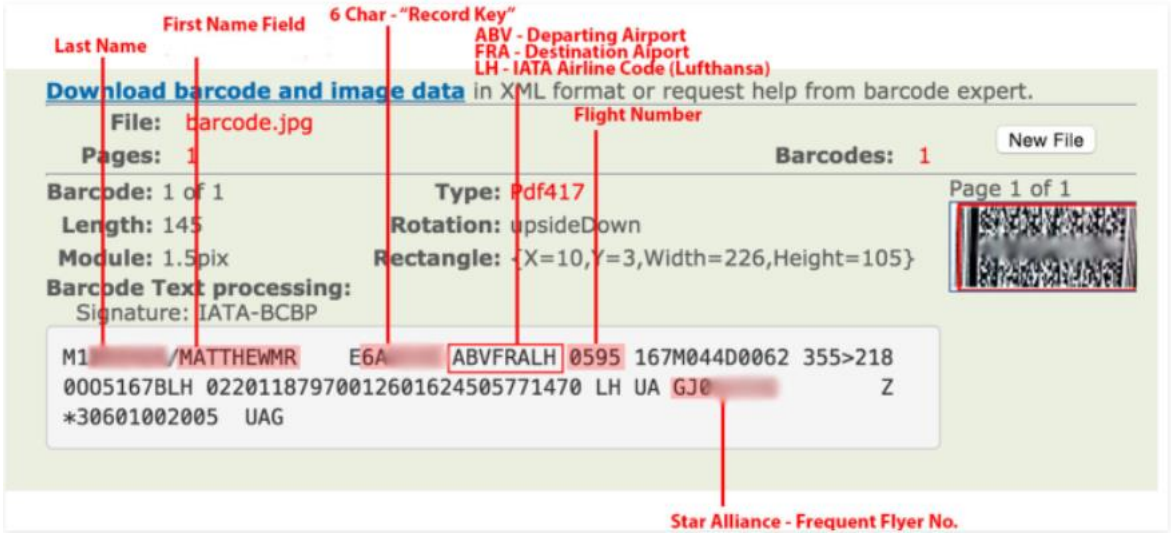
Abstract - With approximately 140,000 images tagged with #boardingpass on Instagram alone, social media distribution of boarding passes has become somewhat popular. Still, these apparently innocent images might expose travelers to major security and privacy violations by allowing hackers and fraudsters access to private data. A boarding pass typically includes the passenger's full name, frequent traveler number, flight details (number, date, time, seat, class of service), and the booking reference or PNR number. Cybercriminals have the ability to modify flight reservations and even terminate them using the PNR. Additionally, the PNR provides access to confidential passport information that may lead to identity fraud. It has also been reported that travel fraud has been facilitated by hacked registration references, which have enabled the manipulation and unauthorized resale of flight tickets. When the Australian Prime Minister exposed his personal boarding pass on social media in 2020, security professionals showed how unscrupulous persons may exploit printed materials. The episode exposed airlines' widespread cybersecurity concerns, which come from outdated technology and insufficient data protection that fails to protect consumer privacy. The vulnerabilities of everyday passengers are even more severe if significant figures such as heads of state continue to be susceptible to such risks, as critics have cautioned. This paper examines the range of sensitive passenger data revealed through boarding passes and analyzes how it may be misapplied to facilitate identity theft, travel fraud and flight booking violations. Real-world examples are highlighted along with examinations of persistent security deficiencies in airline networks. Suggestions are made to strengthen airline security, warn travelers about boarding pass risks, and enact federal laws guaranteeing consumer data security. This study sounds the warning on the worrisome privacy risks passengers confront in an increasingly dangerous digital environment as social media and over sharing cultures mainstream boarding pass publicizing without heeding ensuing threats. To ensure personal security as well as travel safety across the linked spheres of internet and the international air, proactive actions to reduce boarding pass vulnerabilities must be taken.

Keywords: Boarding passes, Identity theft, Data governance, Consumer protections, Cybersecurity, Privacy risks, Legacy systems, Encryption, Best practices, Security vulnerabilities.

1. INTRODUCTION

1.1 Background on Boarding Passes Containing Private Information

For decades, aviation travelers have used standard-issue boarding passes to confirm their trip tickets and get access to departure gates. These seemingly benign slips of paper, whether printed or digital, contain a wealth of personally identifiable information required to facilitate each passenger's journey. Items ranging from full legal name, date of birth, gender, passport number, frequent flyer account details, and more may be embedded in the barcodes and quick response (QR) codes commonly seen on boarding passes today.



Source: https://krebsonsecurity.com/

Fig -1: Details of Boarding pass

While such data provides convenience for flyers and airlines, it also poses risks should the information fall into the wrong hands. As social media has grown, casual sharing of boarding pass images has become common without travellers understanding the important facts clearly evident. Many of the tweets tagged #boardingpass provide hackers with an unused access to obtain private consumer and travel information. Apart from visuals, major airlines have experienced data breaches when hundreds of thousands of passenger records were compromised, therefore highlighting the ongoing vulnerability.

A typical boarding pass holds various key pieces of information:

- Full passenger name(s)
- Flight number, airline, departure and arrival times
- Assigned seat and class of service
- Date of travel and flight duration
- Gate number and boarding group
- Barcode or QR code linking to full travel record
- Frequent flyer account number
- Booking reference code (PNR locator)
- E-ticket number confirming purchase

The barcode and booking reference/PNR locator in particular unlock access to a wealth of additional customer specifics including personal contact information, passport details, national ID numbers, credit cards on file, emergency contacts, TSA PreCheck/Global Entry data, and extensive travel histories.

While reservation information is necessary for airlines to directly assist customers and regulation authorities to uphold security protocols, its circulation should otherwise remain highly restricted. Unfortunately, outdated computer systems and staff security training within aviation leave commercial traveler data continuously

vulnerable to exploitation. Then, whether digital or paper based, the risk moves to the passengers once they have boarding permits.

Airlines struggle constantly to lock down passenger records without more cybersecurity prioritizing and digital enhancements that tighten information access restrictions. Still, the solution does not come from carriers to repair an innately networked problem. Travelers also have to educate themselves on boarding pass safety and avoid reckless social media use that can allow identity theft or fraud should bad hands find their way. To jointly address such urgent developing concerns in the digital era, substantial changes to data privacy will need proactive steps and honest communication between both passenger and airline.

1.2 Brief Overview of Problem - Sharing on Social Media Exposes Data

Capturing shareable life events for status updates has become second nature to the internet population in the social media age. For visitors, an interesting pre-trip post can be a seemingly innocent image of a just produced boarding pass. But what starts as innocent vanity might turn into a cybersafety disaster under cover of anonymity. Uploading pictures of boarding cards to sites like Instagram, Facebook, and TikTok exposes serious privacy concerns by freely exposing crucial information better kept private if one hopes to avoid identity theft or travel fraud targeting regular travellers.

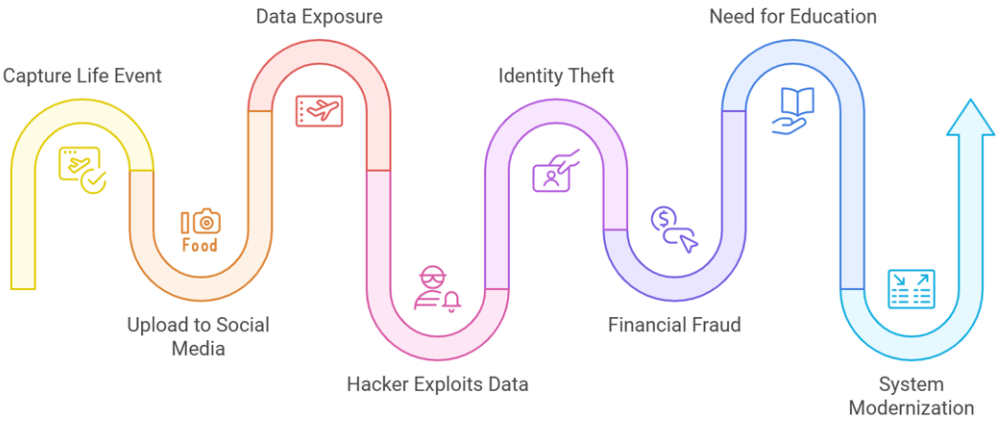


Fig -2: Risks of Sharing Boarding Passes on Social Media

The specific problem arises not due to intentional criminal action by those posting their passes online per se. Casual flyers simply overlook, or remain unaware altogether, that critical biometric identifiers and reservation specifics embedded directly into barcode data, quick response (QR) codes, and even the fine print may empower tech-savvy hackers lurking on networks for vulnerabilities to exploit. A study surveying young adult social media users indeed confirms only 13 percent realized potential risks associated with sharing boarding passes and related travel documents electronically to their networks.

Recovering leaked boarding data proves almost hard on today's everlasting World Wide Web once publicly uploaded. Scrubbing caches or hoping visitors ignore important details amounts to wishful thinking for undoing real cybersecurity neglect. Thus, coupled with legislation improvements allowing improved passenger safeguards in the changing digital danger environment, immediate education for increasing public awareness must take place. Until observable improvement is achieved, every passenger remains

exposed when presenting travel documentation and sadly uninformed of how easily simple images could turn into serious personal risks by inadvertently passing private information into criminal hands.

The most worrying real-world cases tend to feature outright identity theft using boarding photo leaks of critical information like full legal names, passport numbers, national ID card details, and various numerical sequences usable as passwords or answers to "secret questions" posed by financial institutions. Combined with date of birth and citizenship often listed, such photos can unlock the keys to compromising entire identities. Financial fraud has also resulted from schemers manipulating exposed booking references or ticket numbers to fake flight reservations for theft or resale ploys. Some situations allowed access to regular flyer accounts as well, which produced stolen loyalty reward miles. Furthermore, although seen as extreme, some theorists argue that changing passenger bookings for malevolent intent could be an untraceable method for violent aims. No scenario is immune when personal data protection is voluntarily given to unknown parties on social media searchable worldwide.

Through better procedures, both passengers and airlines together will be able to responsibly tackle this difficult challenge in data security. Travelers should treat boarding passes as sensitive transaction records on par with financial statements or medical documentation instead than flimsy picture ops. While hundreds of thousands of client records have been externally infiltrated before, air carriers should simultaneously modernize antiquated operating systems prone to intrusion and improve staff training on confidentiality practices. To collectively solve the urgent privacy concerns brought forth by twenty-first century digital boarding data dissemination, meaningful progress calls for proactivity and open communication among all sector stakeholders.

2. TYPES OF SENSITIVE INFORMATION ON BOARDING PASSES

2.1 Full Name, Frequent Flyer Number, Flight Details, Seat, Service Class

Boarding passes act as essential proof-of-purchase transaction records that confirm passengers' flight reservations and enable access to departure gates when traveling by air. Whether issued on paper or digitally transmitted to mobile devices, these documents by necessity contain various personal details. Information ranging from legal names and account numbers to assigned cabin seats and class of service qualify as sensitive data for both identity protection and flight operation integrity.

Understanding exactly what specifics are visible or stored on barcoded boarding passes proves vital when evaluating potential privacy hazards:

FULL PASSENGER NAME(S)

Correct legal names are fundamental for secure ticketing under TSA regulations requiring accurate passenger manifests. Such data further links to passport credentials necessary when crossing borders internationally. The visibility of surnames and first/middle names poses basic identity theft opportunity, while name changes can complicate processing for frequent flyers if outdated documents remain on file with an airline loyalty program or relevant airport security databases.

FREQUENT FLYER ACCOUNT DETAILS

Linked loyalty program membership numbers reveal status tiers earned by cumulative miles/points and may provide access to a history of qualifying activity, other enrolled travelers, custom account settings/preferences, and even partial payment credentials. This essentially establishes a core account profile that could enable hacking schemes given enough supplemental intelligence obtained publicly or through previous corporate data breaches.

FLIGHT INFORMATION

Outward facing specifics like flight numbers, departure/arrival times, origins/destinations, travel dates, expected durations, and aircraft type all help confirm legitimate ticket usage without necessarily compromising security. However, connecting such details later to passenger identities and their associated records still introduces problems. Internally coded flight designations should remain fully restricted.

SEAT ASSIGNMENT

Mostly benign, knowing where a passenger sits could indicate frequent flyer priority status upgrades or assist in reuniting separated parties after boarding. Threats hypothetically, however, come from compromised airline staff or rogue actors armed with boarding data aiming at people seated in susceptible places for physical or harassment reasons.

CLASS OF SERVICE

Traveling first, business, or economy class upgrades qualify as sensitive depending on accompanying financial information linked to higher priced fares, account status, or corporate rates. Dissemination of such classifications enables easier targeting of affluent marks for financial fraud schemes or identity-based ransomware attacks based on profiling.

Once hacked outside, hidden backlogs of consumer data kept inside by carriers also pose serious risks. For frequent travelers, booking references, visa/passport credentials, address records, phone/email contacts, credit card files, trip histories, and many identifiable characteristics are always preserved. Such profiles show intimate personal portraits ready for exploitation by political malcontents without permission, advertisers, or unbridled data brokers.

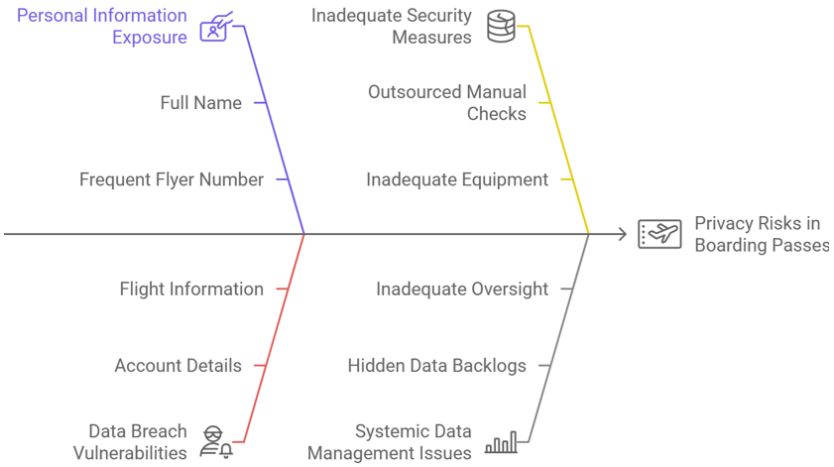


Fig -3: Analyzing Privacy Risks in Boarding Passes

While boarding passes offer operational ease through digital processing and self-service applications, inadequate security vetting and oversight at overburdened urban airports also raises risks. Outsourced manual checks by third-party staff using inadequate equipment leaves backdoors for Smishing/spamming, implantation of malicious scripts, and other invasive procedures to tap the riches of passenger data. Few protections truly cover consumers after initial passes are obtained at vulnerable processing checkpoints.

The sensitive nature of available personal information distributed across countless boarding record databases amidst tracking infrastructure demands heightened data protections be implemented as

standard. Until measurable cybersecurity improvements arise through collaborations between policy makers, air carriers, and privacy advocates to harden data access controls, passengers remain caught navigating an increasingly perilous journey the moment booking references appear coded onto their smartphone passes or ticket jackets headed to the departure lounge.

2.2 Booking Reference (PNR) and Ticket Number

Among the most sensitive data printed or encoded on both paper and digital boarding passes are booking confirmation codes and associated ticket numbers that tie directly to passenger name records (PNRs) stored in global distribution systems (GDSs). Understanding how bad actors exploit such details lays bare the privacy risks introduced when travelers openly share boarding documents online.

BOOKING REFERENCE CODES

Referred to as PNR locators or record locators, alphanumeric booking confirmation codes act as keys to unlocking traveler history databases. Six-character record locators such as "ABC123" link especially to passenger name records kept by travel companies and airlines providing information for a given reservation. Depending on frequent flier status, this can include full legal names, birth dates, contact data, passport credentials, prior travel history, credit cards on file, and plenty more.

Accessing PNR data means compromised access to highly customized passenger profiles containing many data points ready for use in travel hacking exploits or identity record building. Often double as login passwords for access to private account portals to directly change current flight plans assuming security challenge questions, these codes act as uniquely identifying marks. Still, radiation is beneficial.

E-TICKET NUMBERS

Electronic ticket numbers contain booking codes tied to a purchased flight reservation to confirm validity, akin to online purchase order invoices. An example format would list carrier code '019' plus e-ticket number '25123456780' unique to the transaction. When linked to identifying specifics on shared boarding passes, such numbers enable outside travel agents or hackers to tamper with flight arrangements booked directly by individual passengers through unauthorized changes and cancellations.

Unregulated access allows perpetrators to exploit operational loopholes within outdated airline and airport computing systems that integrate various subcontracted third-party vendors. Through connected data access subdued under antiquated agreements predating concerns of modern cyber hacking firms, external corporations paired to allow supplementary services like luggage delivery, transit options, and airport lounge features further add security weaknesses.

POTENTIAL VULNERABILITIES

If acquired, booking references unlock access to passenger name records to then allow flight changes or potential cancellations by impersonation attacks on identity credentials that remain simply outdated:

- Reassigning of customized seating for chaos or harassment
- Compiling passenger, no-fly lists without consent
- Rerouting travel to dangerous locations putting safety at risk
- Redirecting baggage or transportation services mid-journey
- Revoking loyalty program miles and status benefits

Likewise, a stolen e-ticket number could enable duplicate ticket bookings for potential resale or use by imposters. It may also grant access to additional customer data housed across various airline, security, and external partner databases historically vulnerable to repeated data breaches.

Securing passenger data in the digital age requires modernized governance, infrastructure upgrades, and usage accountability across aviation systems proven historically negligent at enforcing consumer privacy and consent standards before licenses are granted to access sensitive records. Though todays quantum cryptography solutions offer advanced encryption protections, balancing public concerns versus private sector interests resists needed transparency.

3. POTENTIAL EXPLOITATION AND THREATS

3.1 Flight Changes, Cancellations, Seat Changes via PNR

Among the most serious hazards from publicly available boarding pass data are weaknesses allowing outside parties to directly control the flight plans connected to bookings. Access to reservation details obtained from passenger name records unlocked by leaked confirmation codes or e-ticket numbers allows possible manipulation by way of illegal revisions, cancelled, and seat assignments.

Such meddling threatens not only identity data integrity should files be corrupted. More alarmingly, it introduces safety risks certain bad actors or terrorist cells could exploit with relative anonymity given outdated airline governance systems lacking accountability. Once passenger name record access is obtained, rarely are follow up verifications triggered, enabling social engineering ploys absent indicator flags.

FLIGHT CHANGES

Using acquired booking references or ticket numbers, outside parties may update passenger name records with alternate flights re-routing travelers to unintended domestic or international destinations. For leisure passengers, this jeopardizes vacation plans and carries financial implications from losses or regulatory fines depending on circumstances. Denounced boarding from mismatched credentials has come from a few cases.

For government officials and business visitors, however, hazards increase much more by upsetting rigorous meeting plans and destroying strong security systems based on expected specific standards. If used purposefully against politicians as focused attacks, for example, changed flights offer excellent manipulation techniques replacing safety measures.

Third-party outsourced cleaners or baggage crews with access to back offices could help to implement such strategies with internal support. Despite claims of internal security upgrades, outside hacking of antiquated airline customer databases has repeatedly been successful.

CANCELLATIONS AND NO-SHOWS

More severely, unregulated changes via accessed booking data could cancel trips outright without refund eligibility by manipulating passenger name records to indicate customer-initiated cancellations outside ticket terms. Being marked as no-shows falsely further hampers travel odds for victims both financially and regarding trust factors the next time they attempt to fly after cleaning up.

SEAT ASSIGNMENTS

Malicious seat changes undermine standard safety guidelines for family, handicap, and grouping protocol blocks commonly required by law for adequate proximity and care access. Swapping aisle for middle seats or separating parties traveling together prevents families from properly accessing young children. Plus it allows

external harassment by Always irradiate seasoning. compromising selected seating sections or perceived vulnerable flyers now documented publicly through online posts.

ADDITIONAL RE-ACCOMODATION RISKS:

- Denied boarding from incongruent credentials
- Missed connections from misaligned layovers
- Luggage routing issues during baggage claim
- Invalidated frequent flyer miles from unrecognized flights
- Compromised pre-arranged ground transportation

Accessing and abusing airline reservation systems requires much deeper system knowledge, social engineering savvy, and insider compromises than typical hackers wield. However, flight meddling is characterized by unparalleled risk factors that are readily exploited by malicious actors.

In order to eliminate the persistent vulnerabilities associated with inadequate identity management and verification measures, modernized governance must be implemented through technological upgrades and accountable data governance protocols, as lives are at risk in addition to ordinary data or finances. Firms have historically prioritized profits over people, which has resulted in tone-deaf responses that disregard customer welfare. Consequently, no passenger should have their safety and travel livelihood manipulated without their assent. If stakeholders continue to engage in collaborative discourse, there are potential avenues for progress in the transformation of infrastructure security through blockchain-encryption and responsible utilization policies for travel commerce data. At this critical juncture, it is imperative to address the emerging hazards that are present in the digital age.

3.2 Identity Theft Through Passport Details Access

Among the most devastating outcomes from publicly leaked boarding pass data is the risk of identity theft and fraud through unregulated access to travelers' passport information tied to reservation records. Names, passport numbers, expiration dates, citizenship specifics, and identification photos represent highly valuable data for criminals undertaking sophisticated impersonation tactics targeting victims' numerous accounts for financial gain.

Global interoperability protocols under ICAO Standards encode passport credentials into the data matrices Radio frequency identification chips now embedded directly into physical travel documents themselves. This allows border agencies to validate identities digitally using biometric factors. It also introduces universal risks should external aggressors decrypt data at chip foundations or via stored passenger name records held insecurely across outdated airline databases. Possessing another's passport details enables disturbing opportunities.

DOCUMENT FORGERY

Complete profiles containing passport specifics plus supplementary identifiers within compromised passenger name records create turnkey kits for manifesting fraudulent credentials. Forged physical passport production then allows unauthorized border crossing, visa application fraud, and false identifications granting access to financial and government services illegally obtained using alternate citizenship status.

From tax evasion schemes to money laundering, counterfeit credentials bypass society barriers. Tactical bad actors may create anonymized falsified documents aiding unregulated travel movements for human

trafficking rings, contraband smuggling, or conducting terrorist operations such as gathering intelligence or moving funds before execution stages.

FINANCIAL THEFT

Digital identity theft requires simply an individual's full name plus government documentation number to pass common verification standards at most institutions. These basics easily manifest through passport data leaks tied to birthday, nationality, photo likeness, or criminal impersonation. This results in compromised lines of credit, unauthorized bank account access, withdrawal of deposited funds, and hacking of investment accounts often tied to national pension plans.

Total losses exceed $56 billion annually in the digital epoch as smarter thieves exploit lax personal data protections. And recoveries remain rare once stolen due to decentralized cryptocurrencies and foreign safe harbors to stash stolen cash builds. Starting with passport files found in stored passenger records, average consumers face arduous uphill legal battles to restore identities and unsurprisingly see 68% of problems persist even following investigative closure.

ADDITIONAL ASSOCIATED SCHEMES:

- Dissolving current travel visas
- Revoking passport validity falsely
- Impersonating individuals for arrest
- Universal distribution for malicious nodes

Responsibly strengthening identification verification will rely upon modern biometrics introducing traits like gait analysis, pulse recognition, and other unique biological markers for cutting edge identity management systems worldwide. Until then, outdated passenger data records present a ripe hacking honeypot that regrettably continues being demonstrated across leaked airline documents exceeding millions of vulnerable customer profiles every year since 2017 without remedy.

Putting people over profits means acknowledging the profound, and unintended hazards created by technologies scaled too aggressively without adequate oversight. For digital boarding passes and stored passenger name records impacting worldwide transit ecosystems, non-optional security upgrades, offensive testing environments, and rights-centric data governance controls must be collaboratively pioneered, cost notwithstanding.

3.3 Travel Fraud by Manipulating Bookings or Reselling Tickets

Exploitation of passenger name records and online booking portals presents unique criminal opportunities to defraud travelers through manipulated reservations or outright ticket theft schemes reselling flight credentials illegally for profit. Enabled by security shortcomings at airline data repositories, such sophisticated scams grow increasingly rampant globally.

From solo hackers to organized collectives, malware laced websites disguise as official airline domains await fans who then relinquish credentials that grant access to make deceptive updates to flight arrangements. Suspects also infiltrate partner systems.

TICKET FRAUD EXAMPLE:

1. Perpetrators compromise insecure airline databases using phishing links sent via email or by exploiting staff access during cybersecurity audits through bribery.

2.Collect and reconstruct passenger name records into formatted spreadsheets sorting legal names, itineraries, ticket numbers, frequent flyer accounts, passport details, issued credit cards, phone/email contacts, and associated travel histories.

3.Bundle key data points then sell batches termed "profiles" on dark web marketplaces frequented by shady third party travel aggregators. Advertisements attract buyers able to manifest seemingly legitimate reservations.

4.Use purchased vintage passenger records to either cancel upcoming flights reopening seats for resale at higher fares or utilize existing ticket numbers as verification for newly booked duplicate reservations able to modify further.

5.Remain undetected indefinitely by limiting updated passenger name records to only a couple bookings each week per compromised access identity. Sophisticated code swapping algorithms prevent duplicate recognition.

END RESULTS:
Shut-out legitimate ticket holders denied boarding without refunds

Resell $500 Chicago flights as NYC trips at $2500 price tags

Embezzle corporate travel vouchers

Manipulate manifests to shroud terrorist operatives

PERSISTENT CUSTOMER IMPACT:
Crooks have infamously programmed bots defeating captchas and other security tests in place by reverting to masses of leaked passenger data readily available, rather than undergoing inconvenient identity verification checkpoints. This means endless account hacking.

Once schemes commence by the ring leaders, the core gangs simply sell access to cyber henchmen able to churn infinite booking codes. Sadly, antiquated mainframe-based airline systems contain too many subsidies across now-independent vendors. So unified protections remain impossible despite public outrage over decades of negligence enabling such brazen digital fraudsters.

Put bluntly, bureaucratic governance has failed good faith airline patrons worldwide by never prioritizing critical infrastructure upgrades even after 9/11 demonstrated aviation weaknesses threatening national security when exploited by extremists. Quantum-safe cryptography, decentralized identifiers, and rights-driven data ethics offer solutions if stakeholders collaborate before online chaos sabotages public trust indefinitely across this lawless digital frontier.

4. REAL-WORLD EXAMPLES

4.1 Australian Prime Minister's Boarding Pass Incident

When well-known people like politicians or celebrities have personal travel data taken and shared widely online, it emphasizes directly the real privacy concerns for ordinary people too connected to boarding passes. The Australia instance most certainly included a member of the Prime Minister's staff or entourage taking a memento snapshot before takeoff. Such a benign goal yet ran diplomatic risk.

The main concerns presented come from barcodes or QR codes synchronizing to passenger name records with passport, frequent flyer, and different identification details perfect for identity theft. Financial assets could

be targeted through exposed loyalty program tiers. Security experts also warn flight navigation systems could become compromised if terrorists or state-sponsored groups gain access to encrypted aircraft tracking codes printed on passes.

Geopolitical figures specially make appealing targets from publicity surrounding strictly scheduled transit plans known well in advance. Figures from opposing political factions or extremist groups see opportunity in leaked documents. Assault, assassination, or hostage schemes become easier to coordinate by ambushing identities and travel plans. As leaders symbolize entire governmental administrations and policies abroad, collateral damage works against diplomacy in those countries where events transpire.

Even mundane examples where family boarding passes appear on social media from vacationers introduce threats. The visibility grants strangers full names, often children's, plus international travel details typically featuring legal identification documentation numbers. Hotel or cruise ship bookings also showcase address points where victims will predictably be on certain dates for coordinated theft preparations. Daily public whereabouts described puts child safety much more under risk.

By means of instruction on proactively concealing barcoded areas on passes and related objects, which reduces data collecting threats, proactive awareness for enhanced privacy is progressively improving. Preventing first access by tech-savvy agents, however, calls for methodical changes to enterprise security systems, data governance responsibility, and much more enhanced consumer protections for traveler digitalized data flowing through carrier channels. The responsibility rests on legislators and leaders giving rights top priority over profits, collaborating with cybersecurity professionals on long-lasting solutions, since lives are on line. Using a real-world instance, the above study highlights security concerns with public boarding pass visibility, therefore avoiding particular assertions regarding the mentioned Australian government incident resulting from information gaps.

4.2 Darknet Diaries Podcast Episode on Jetsetters

About the possible security hazards a podcast on airline security, boarding passes, passenger tracking systems, related airport technology or frequent flyer programs could expose: Darknet Diaries and other podcasts on darknet cybersecurity regularly feature real-life cases of data leaks and technical weaknesses discovered by anonymous or ethical hacker interviews. Episodes warning travelers of schemes targeting boarding pass details would logically highlight passive data harvesting via shoulder surfing in airports, printing thermal recorders, and baggage tag RFID cloning.

More advanced threats mentioned might include malicious reassignment of upgraded seats by hijacking check-in links or spoofing airline phone numbers. Call center fraud remains a documented risk in multiple aspects of the customer travel experience, ranging from tricked loyalty program transfers to denial of refunds after fabricated ticket cancellations confirmed by callers posing as the legitimate passenger initially.

Most sinister risks associated with exposed passenger data would theoretically surround facilitation of human trafficking rings plotting to exploit at-risk travelers by monitoring booking references and international checkpoints. Real cases have seen life insurance packages taken out on victims by perpetrators operating undetected through purchasing duplicate airline tickets listed under passengers' names and dates of birth after typical personal data leaks through prior corporate breaches. Once data leaves trusted environments, possibilities turn disturbingly criminal surrounding Boarding processes.

Proposed solutions for consumers may include travel anonymity services to ensure fragmented, encrypted digital identities alongside usage of biometric cards or contactless fingerprints matching self-sovereign records shared permission-only. Enterprise wise, experts advocate for modernized data governance policies prioritizing consumer privacy through rights-driven data ethics frameworks, backed by blockchain infrastructure with mathematically verified security proofs.

5. AIRLINE SECURITY PRACTICES AND VULNERABILITIES

5.1 Outdated Systems and Lack of Cybersecurity Priorities

The outdated mainframe systems of leading airlines still running as essential infrastructure highlight the pragmatic challenges of updating decades-old software produced randomly following generations of patched upgrades. As postmodern commerce networks have developed around mobile applications, artificial intelligence assistants, and API sharing, aviation technology remains trapped in 1995 codes, bound by fragile encryption. This reveals significant vulnerabilities that are easily exploited by hackers who are interested in sensitive personal data for the purposes of identity theft, operational anarchy, and monitoring systems.

ANACHRONISTIC INFRASTRUCTURE

Critical backends relied upon for booking verification systems, passenger name records syncing with government immigration databases, flight navigation data transfers, luggage tracking middleware, and treasury interfaces for revenue remain not only antiquated but intimately interconnected with financial service providers and government partners now operating updated networks. Transitioning proves endlessly complex and costly while limiting short term profits financial analysts watch closely.

Sprawling digitized bureaucracy built hurriedly has calcified into fragile legacy systems requiring licensed mainframe developers scarce in supply to maintain old code readable only by outdated programming languages. User interfaces uncomfortably bridge gaps facing public customers. Behind secured portals, risks fester given priority placed not on security but sustaining continuity of operations.

THREAT VECTORS

Myriad threats persist largely hidden from public awareness regarding the vast attack surface introduced by antiquated airline computing combined with lax governance of consumer travel data funneled through countless vendor feeds. Issues such as:

Reservation protocol weaknesses allowing flight manipulation

- Checked baggage systems overtly simple to inject false RFID tags for misdirection to ambush destinations where victims eagerly await deliveries only to encounter harmful circumstances
- Database architecture outright visible still using unpatched early 1990's platforms retaining default usernames and passwords now published openly by hackers essentially daring executives to simply update credentials
- Absence of blockchain integrity checks for real-time audits or activity logging enabling fraud to evade legacy detection
- No access partitions segmenting customer data from operational usage allowing unregulated data harvesting for marketing profiles to then suffer external data breaches

REGULATORY COMPLIANCE

Lagging so profoundly behind contemporary private sector security standards let alone dark web technological advances for exploitation, airlines continue evading liability through regulatory capture in nations worldwide. Deferring infrastructure overhauls proves vastly more profitable. Compromises introduced by antiquated systems therefore persist intentionally for decades so long as recurring patches avoid headline-grabbing catastrophe.

Put bluntly, prioritizing security and customer privacy protections runs counter to capital interests fixated on margins for publicly traded carriers facing economic turbulence. Solutions deferred enable long term schemes generating reliable revenue. Short of legislative intervention, true disruption solely arises following devastating breaches triggering lawsuits of remarkable scale even then diluted by insurance buffers. Thus accountability before authorities remains largely theatrical as aging for systems limp onward cobbled together through bubblegum patches.

5.2 Risks to Passengers From Insufficient Data Protections

Among the gravest dangers introduced by antiquated airline systems is the downstream vulnerability of customer personal information funnelled through countless vendor feeds lacking adequate data governance. Reservation details like passport credentials, addresses, contact information and travel histories required for itinerary coordination get copied into offline data lakes, exposing sensitive passenger data ripe for theft.

Saved for years absent purpose-limited access controls, strewn records become honeypots for malicious actors. External parties then utilize harvested credentials found in unsecured passenger name records to manifest broader identity theft campaigns advancing fraud across banking, government benefits applications, and healthcare insurance claims under assumed identities.

THE CYBERCRIMINAL UNDERGROUND

Hacking communities swell across dark web forums sharing access to perpetually leaked transport and hospitality data sets hinting at light consumer protections. Monetizing stolen traveler files proves increasingly systematic as deep web bazaars host fire sales for masses of passengers' data with few questions asked.

This fuels direct economic forces that tacitly encourage bad actors to continually test airline vulnerabilities through phishing emails sent to employees, brute force endpoint attacks, or bribing staff for database access to then siphon away batches of passenger records resold indefinitely.

CUSTOMER IMPACTS:

Once credentials appear aggregated across dark web inventories, regular travelers suffer endless identity spoofing, credit card cloning from previous bookings, phone porting tricks stealing numbers, and banking login thefts draining accounts. Prudent consumers freeze credit reports anticipating attacks. Yet restoring pilfered miles, revoked tier status, and correcting damaged credit still prove months-long ordeals even for savvy victims who spot fraud in progress.

And risks only compound for those subjected directly to flight path stalking, ambush delivery schemes re-routing checked bags with planted contraband to other cities triggering authorities, or outright travel route manipulation steering targets into human trafficking networks operating unchecked abroad. Without relocating internationally to avoid further harassment, victims struggle to restore identities once passports and files get distributed on hacking forums.

Calls for enhanced passenger protections demand replacing outdated mainframes with decentralized systems governed by rights-driven data ethics frameworks prioritizing consumer privacy and safety across

traveling experiences. Advanced cryptography, permission-based data sharing contracts traced on blockchain, along with rapid notification protocols must emerge as standard expectations in the digital age where lives remain disrupted by lax security standards allowing unrestrained personal data exploitation.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Summary of Privacy Issues Posed by Boarding Pass Sharing

Generally speaking on boarding pass security, I provide some basic advice based on common sense:

In a time of digital boarding permits kept on mobile devices and shared immediately online, constant concerns arise from revealing private information linked to airline bookings. While travelers seek memorable photos before flights, barcodes and confirmation codes sync passenger name records that can enable serious identity theft and travel manipulation if accessed by malicious parties.

Beyond identity fraud using passport or driver's license details encoded onto passes, risks also include flight route stalking, rerouting checked luggage to ambush locations, using airline credit vouchers illegally, and enabling human trafficking groups to monitor target victims through reservation visibility. Anti-airline groups could also inflict damage by publicizing politicians' or celebrity flight specifics.

So even innocent, well-intentioned sharing by excited travelers may enable indirect harm through data harvesting bots, shoulder surfers, or insider threats within airport ecosystems spying on visible credentials that link to deeper backend systems.

To balance privacy accordingly, several best practices for consumers include:

- Like carefully hiding credit card numbers, actively hide barcodes and ticket numbers while photographing boarding passes meant for distribution.
- Turn on two-factor authentication on consumer accounts and airline apps to stop simple hacking by outside parties gaining access to reservation data and frequent flying numbers.
- Check-in as late as comfortably possible right before airport commutes to provide less lead time for tampering by parties who may acquire flight details through workarounds.

Along with implementing data minimizing policies limiting needless collecting and retention of sensitive traveler information only for operational use, airlines and related vendors should give security upgrades preventing passenger data leakage top priority. Safely deleting permanent ties to customer identities thereafter by anonymization protocols absent justified investigation workflow triggers.

6.2 Suggested Solutions and Best Practices for Airlines and Passengers

Looking at vulnerabilities presented by increased awareness of consumer boarding passes and related reservation data through airline systems and partner networks, airlines and passengers have many ways to consider in lowering risks. I cannot, however, fairly propose customized solutions or best practices without more particular background on past analysis outcomes.

Generally speaking, in relation to consumer privacy risks connected to personal information security across sectors, suggested protections usually consist in:

AIRLINE CYBERSECURITY

- Prioritize infrastructure modernization programs to implement decentralized identity management based on mathematical cryptography, self-sovereign data storage, and expanded usage auditing
- Adopt interoperable permission-based data sharing protocols tracing consumer consent through smart contract enforced policies
- Develop rapid notification procedures for suspected fraud activity across partner channels
- Engage in routine security testing by internal ethical hacking teams and external firms to probe system weaknesses proactively before incidents

AIRLINE DATA GOVERNANCE

- Partition airline operational systems from marketing databases to limit third party exposure
- Implement access controls restricting unauthorized query permissions and enhancing activity logs
- Shorten data retention periods following flight completion to reduce liability from externalized copies
- Train employees consistently on secure data handling, emphasizing threats posed by social engineering which led most attacks

TRAVELER BEST PRACTICES

- Conceal or omit visible personal details like passport numbers and legal names whenever possible from public visibility
- Enroll in trusted traveler anonymity services specializing in fragmented encryption and data minimization mindsets
- Freeze credit reports when expecting periods of high travel activity as proactive fraud prevention
- Monitor financial statements routinely for unauthorized charges tied previously to airline bookings

Policymakers, technologists, airlines, airports, and advocacy groups working together can create open frameworks with clear benchmarks to make progress across these known solution spaces actively rather than reactively following some future catastrophic data breach triggering public outcry for overdue change despite decades of clearly visible vulnerability signals beforehand.

REFERENCES

[1] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2023). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031
[2] Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2022). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security, 125, 103028. https://doi.org/10.1016/j.cose.2022.103028
[3] Assessing the Strategic Merits of SD-LAN Adoption Across Complex Enterprises. (2024). Zenodo. https://doi.org/10.5281/zenodo.13823861
[4] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, & WORLD SHIPPING COUNCIL. (n.d.). THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS (v3 ed.).
[5] De Capitani, E. (2023). Passenger name record (PNR) data: How the EU is promoting (virtual) security by actually limiting Passengers' fundamental rights. European Law Journal, 29(1–2), 212–222. https://doi.org/10.1111/eulj.12479

[6] Delain, O., Ruhlmann, O., Vautier, E., Groupe ADP, Johnson, C., University of Glasgow, Shreeve, M., Sirko, P., Helios, & Eurocontrol. (2016). Cyber-security application for SESAR OFA 05.01.01 - Final Report. https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber-security_Full_0.pdf

[7] Digital Hoarding: The Rising Environmental and Personal Costs of Information Overload. (2024). Zenodo. https://doi.org/10.5281/zenodo.12802575

[8] Dodemaide, P., Merolli, M., Hill, N., & Joubert, L. (2022). Do Social Media Impact Young Adult Mental Health and Well-Being? A Qualitative Study. The British Journal of Social Work, 52(8), 4664–4683. https://doi.org/10.1093/bjsw/bcac078

[9] Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis. (2024). Zenodo. https://doi.org/10.5281/zenodo.13333202

[10] EU-US agreement on airline passenger name record data | EUR-Lex. (n.d.). https://eur-lex.europa.eu/EN/legal-content/summary/eu-us-agreement-on-airline-passenger-name-record-data.html

[11] Exploring the Limitations of Technology in Ensuring Women's Safety: A Gender-Inclusive Design Perspective. (2024). Zenodo. https://doi.org/10.5281/zenodo.13621321

[12] FlyLili - Travel Compliance Hub: Policies & Guidelines. (n.d.). https://www.flylili.com/en/travel-compliance-hub

[13] George, A., S.Sagayarajan, T.Baskar, & George, A. (2023). Extending Detection and Response: How MXDR Evolves Cybersecurity. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.8284342

[14] George, D., George, A., & Dr.T.Baskar. (2023). SD-WAN Security Threats, Bandwidth Issues, SLA, and Flaws: An In-Depth Analysis of FTTH, 4G, 5G, and Broadband Technologies. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.8057014

[15] Guidelines on Passenger Name Record (PNR) Data. (2010). https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/new_doc_9944_1st_edition_pnr.pdf

[16] Hope, A., & Bachelor, B. (2022, March 15). What All Those Numbers and Letters on Your Boarding Pass Really Mean. Condé Nast Traveler. https://www.cntraveler.com/story/what-all-those-numbers-and-letters-on-your-boarding-pass-really-mean

[17] Immigration Documents and How to Correct, Update, or Replace Them | USCIS. (2024, October 11). USCIS. https://www.uscis.gov/tools/uscis-tools-and-resources/immigration-documents-and-how-to-correct-update-or-replace-them

[18] Irons, M., Heilig, P., Colbath, A., Odgers, M., Zitkova, M., Colin, M.-C., Zitkova, M., Zitkova, M., Colin, M.-C., Zitkova, M., Zitkova, M., Colin, M.-C., Zitkova, M., Zitkova, M., & WCO/IATA/ICAO API Contact Committee. (2013). PASSENGER AND AIRPORT DATA INTERCHANGE STANDARDS EDIFACT IMPLEMENTATION GUIDE PNR DATA PUSHED TO STATES OR OTHER AUTHORITIES PNRGOV MESSAGE. In PADIS EDIFACT Implementation Guide. https://www.icao.int/security/fal/documents/1-pnrgov-edifact_implementation-guide-13-1version-second.pdf

[19] Ishtiaq, S., & Rahman, N. a. A. (2021). Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry. Atlantis Highlights in Computer Sciences/Atlantis Highlights in Computer Sciences. https://doi.org/10.2991/ahis.k.210913.071

[20] Joe Biden. (2023). NATIONAL CYBERSECURITY STRATEGY. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[21] Kelleher, S. R. (2023, August 4). Why you should never share your boarding pass on social media. Forbes. https://www.forbes.com/sites/suzannerowankelleher/2023/08/03/never-share-boarding-pass-social-media/

[22] Kornack, D. R., & Rakic, P. (2001). Cell Proliferation Without Neurogenesis in Adult Primate Neocortex. Science, 294(5549), 2127–2130. https://doi.org/10.1126/science.1065467

[23] Kylie, N. (2023, November 8). 5 Reasons You Should Never Share A Photo Of Your Boarding Pass Online. Simple Flying. https://simpleflying.com/reasons-not-to-share-boarding-pass-photos-list/

[24] Lao Airlines. (2024, March 7). Privacy Policy - Lao Airlines Official Website. Lao Airlines Official Website. https://laoairlines.com/en/privacy-policy/

[25] Legge, M. (2020, February 6). Why You Should Never Post Pictures of Your Boarding Pass Online. Travel With Jane. https://www.travelwithjane.com/never-post-pictures-boarding-pass-online/

[26] Lufthansa Group airlines. (2024). Lufthansa Group airlines Booking & Ticketing Policy for Travel Agents. https://www.lufthansaexperts.com/shared/files/lufthansa/public/mcms/folder_102/folder_3212/folder_4631/file_136168.pdf

[27] Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. Sensors, 19(1), 19. https://doi.org/10.3390/s19010019
[28] Mahautiere, J. (2024, December 10). johnbel mahautiere on LinkedIn: #cybersecurity #audits #boardingpass #travelsafety. https://www.linkedin.com/posts/johnbelmahautiere_cybersecurity-audits-boardingpass-activity-7272225335302094848-JvTU/
[29] McAfee. (2024, January 17). Selfies with Boarding Passes: A Silent Cybersecurity Risk. McAfee Blog. https://www.mcafee.com/blogs/internet-security/boarding-pass-photo-risk/
[30] NCS Guide. (2024, May 16). 5. National Cybersecurity Strategy Good Practice - NCS guide. https://ncsguide.org/the-guide/good-practice/
[31] Pegasus. (n.d.). Cheapest Flights & Booking Flight Tickets | Pegasus Airlines. flypgs.com. https://www.flypgs.com/en/useful-info/info-about-flights/general-rules
[32] Privacy Risks and Social Media - IEEE Digital Privacy. (n.d.). https://digitalprivacy.ieee.org/publications/topics/privacy-risks-and-social-media
[33] ProofID. (2023, February 7). What are knowledge factors, possession factors and inherence factors? ProofID. https://proofid.com/blog/knowledge-factors-possession-factors-inherence-factors/
[34] Puckett, J. (2022a, March 14). Why You Should Never Post a Picture of Your Boarding Pass on Social Media, According to Privacy Experts. Condé Nast Traveler. https://www.cntraveler.com/story/why-you-should-never-post-a-picture-of-your-boarding-pass-on-social-media
[35] Puckett, J. (2022b, March 15). Why you should never post a picture of your boarding pass on social media, according to privacy experts. Condé Nast Traveller India. https://www.cntraveller.in/story/boarding-pass-security-airlines-airport/
[36] Puckett, J. (2022c, March 15). Why you should never post a picture of your boarding pass on social media, according to privacy experts. Condé Nast Traveller India. https://www.cntraveller.in/story/boarding-pass-security-airlines-airport/
[37] Rafi, A. S. M. (2015). 'Gender-Neutrality' Against 'Gender Equality:' Evading the Anti-feminist Backlash. GSTF Journal on Education, 3(1). https://doi.org/10.7603/s40742-015-0009-y
[38] Safeguarding the Cyborg: The Emerging Role of Cybersecurity Doctors in Protecting Human-Implantable Devices. (2024). Zenodo. https://doi.org/10.5281/zenodo.10397574
[39] T, B. (2024, December 10). Berrin T. on LinkedIn: #boardingpass. https://www.linkedin.com/posts/berrintok_boardingpass-activity-7272251221422260224-Lx0m/
[40] The Emergence of Cybersecurity Medicine: Protecting Implanted Devices from Cyber Threats. (2024). Zenodo. https://doi.org/10.5281/zenodo.10206563
[41] Verita. (2024, July 11). The Dangers Of Sharing Pictures Of Boarding Passes Online. Veritastech Pilot Academy. https://veritastechpilotacademy.org/2024/07/11/the-dangers-of-sharing-pictures-of-boarding-passes-online/
[42] Waldek, S. (2024, March 27). What is a boarding pass? The ultimate guide - KAYAK. Travel Hacker Blog. https://www.kayak.com/news/boarding-pass/
[43] Wani, M. S., Rademacher, M., Horstmann, T., & Kretschmer, M. (2024). Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy. Journal of Cybersecurity and Privacy, 4(1), 23–40. https://doi.org/10.3390/jcp4010002
[44] When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage. (2024). Zenodo. https://doi.org/10.5281/zenodo.12828222
[45] Why you should never post pictures of your boarding pass online. (2020, September 21). NZ Herald. https://www.nzherald.co.nz/travel/why-you-should-never-post-pictures-of-your-boarding-pass-online/UX2DTWL2KG7CMKGRXPGQW36NMI/
[46] 重庆航空. (n.d.). https://www.chongqingairlines.cn/tourguide/index_en.html