Why Throwing Away Your Old Boarding Pass is so Risky - InfoSec Resources

tags: ✎

It's the holiday season and probably most of you will travel during the Christmas time. For this reason, I decided to propose again a topic that was in the headline a couple of months ago. Do you leave the boarding pass used for air travel anywhere after a trip? Do you know how much information it contains? Probably you are thinking, "If Pierluigi is asking me that, there is something to take care" … correct.

As we have seen, the old boarding pass may contain a lot of personal information that could be used by ill-intentioned against us, so don't throw away your old boarding pass!

After a trip the boarding pass becomes useless, but does that mean that we should throw it in the garbage? Taking a look to a boarding pass, you will notice the presence of a barcode, so let try to understand what information it contains and how a hacker could use it for illegal activities.

In October, the popular investigator Brian Krebs published an interesting post that explained the information stored in a boarding pass barcode.

The airlines use the boarding pass barcode for every single boarding pass. It contains a lot of data that could be read easily by everyone.

Brian Krebs reported the attempt made by one of its readers, a guy named Cory, who saw a friend posting his boarding pass on Facebook.

Cory, intrigued by the friend's post, began to search on the Internet some websites that could help him interpreting the boarding pass and he found what he was looking for.

The boarding pass barcodes are widely available for years. The International Air Transport Association (IATA) published a detailed **document** to explain how the barcode standards have been implemented by the organizations in the industry.

The Passing Board has been around since 2005 when the IATA launched a five-year project to deploy Bar Coded boarding passes (BCBP) across its member airlines. The project aimed to eliminate magnetic boarding passes, a change would allow the industry to save

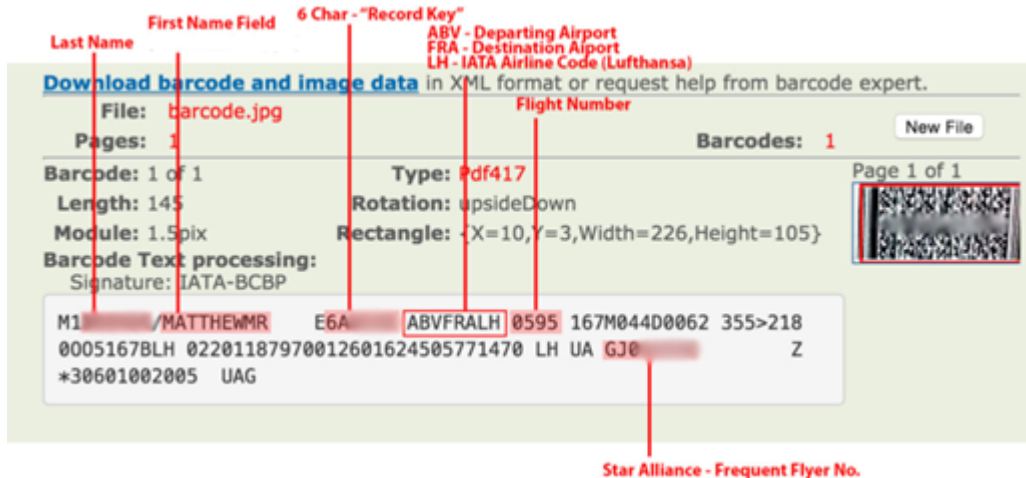US$1.5bn annually and the possibility to enable new technologies such as web and mobile check-in.

Figure 1 – boarding pass

"*I found* __*a website*__ *that could decode the data and instantly had lots of info about his trip,*" *said Cory, "Besides his name, frequent flyer number and other [personally identifiable information], I was able to get his record locator (a.k.a. "record key" for the Lufthansa flight he was taking that day," "I then proceeded to Lufthansa's website and using his last name (which was encoded in the barcode) and the record locator was able to get access to his entire account. Not only could I see this one flight, but I could see ANY future flights that were booked to his frequent flyer number from the* __*Star Alliance*__ *."*

I used the same website discovered by Cory to read data present on an old boarding pass barcode I left in a book, I was surprised by the information I retrieved. It is frightening what someone could do with the information present on a boarding pass, and an Internet connection.

Cory used the info available in the barcode posted online by his friend to enter in the Lufthansa website and access his data, including the phone number and the name of the person who did the booking. In and same way Cory was able to see future flights connected to the frequent flyer account.

Probably for the majority of people, the disclosure of this data doesn't represent a threat, but let start thinking like a hacker. How can we use this information? Is it possible to use it in a targeted attack?

The response is affirmative. An attacker can use the data discovered by Cory to launch a __spear phishing__ attack to the victim. The first attack scenario that comes my mind sees the victim receiving a phishing email reporting information on his flights. The email tricks the victim into revealing additional information, signing a bogus website controlled by attackers, providing financial information or visiting a website that is used to serve a

malware.

In the specific case described by Cory, the man was able to access the list of future flights of his friend, he was also able to cancel them or change seats.

Cory discovered that an attacker could also reset the PIN associated with Star Alliance frequent flyer account, then he tried to use the "Forgot Pin" reset and his friend question was, "What is your Mother's maiden name?"

Such kind of recovery procedure is quite easy to bypass; we disclose an impressive amount of data online such as our mother's maiden name. Digging into social media it is simple to find a message or a picture that could reveal it.

This is just an example of what can be done with a barcode, and the amount of information it can be extracted. Often people consider that the information revealed is harmless, but it is because they don't think like a criminal.

*"Interested in learning what's in your boarding pass barcode? Take a picture of the barcode with your phone, and upload it to **this site** . **This blog** on the same topic from several years back includes some helpful hints on how to decode the various information fields that get dumped by the barcode reader."* **States** Brian Krebs.

What information is available on a boarding pass? I have found an interesting post published by the expert Shaun Ewing, who found out more information on the barcode standard, and the information barcodes contain. Ewing analyzed a number of boarding passes available online by using freely available software utilities to decode the barcodes they contain.

In his post, Ewing used a boarding pass related to a Qantas flight, he decoded the barcode on the web check-in document extracting the following string:

M1EWING/SHAUN MR 1A11A1 BNESYDQF 551 107Y26J 37 00

- He the n parsed the string discovering which info were associated:
- M1: Format code 'M' and 1 leg on the boarding pass.
- EWING/SHAUN MR: His name.
- 1A11A1: Hei booking reference.
- BNESYDQF: Flying from BNE (Brisbane) to SYD (Sydney) on QF (Qantas).
- 551: Flight number 551.
- 107: The Julian date. In this case 107 is April 17.
- Y: Cabin – Economy in this case. Others including F (First) and J (Business).
- 26J: His seat.
- 37: His sequence number. In this case he was the 37th person to check-in.

- 00: Field size of airline specific data message. 00 as there isn't any.

Now that he succeeded in translating the information stored in the boarding pass he decided to analyze another real boarding pass issued at the airport. Below the information extracted from the barcode.

```
1 M1EWING/SHAUN      E1AAAAA SYDBNEQF 0524 106Y023A0073 359&gt;2180
2   B          29        0   QF 1245678          128
```

That translates into:

- M1: Format code 'M' and 1 leg on the boarding pass.
- EWING/SHAUN: My name.
- E1AAAAA: Electronic ticket indicator and my booking reference.
- SYDBNEQF: Flying from SYD (Sydney) to BNE (Brisbane) on QF (Qantas).
- 0524: Flight number 524.
- 106: The Julian date. In this case 106 is April 16.
- Y: Cabin – Economy in this case. Others including F (First) and J (Business).
- 23A: My seat.
- 0073: My sequence number. In this case I was the 73rd person to check-in.
- 3: My "passenger status".
- 59: There is a various size field. This is the size
- >: Beginning of the version number
- 2: The version number.
- 18: Field size of another variable field.
- 0: My check-in source.
- B: Airline designator of boarding pass issuer.
- 2: Another variable size field.
- 9: Airline code.
- 0: International document verification. '0′ as I presume is not applicable.
- QF: The airline my frequent flyer account is with.
- 1245678: My frequent flyer number.
- 128: Airline specific data.

Ewing also discovered that that the same information is used by the mobile boarding pass. The boarding pass documents are a mine of data. Also in this case, Ewing highlighted possible abuses of this information. For example, the booking reference could be used by ill-intentioned to manipulate the owner's booking.

Security Awareness Whitepaper

Michael Born, security expert at the Solutionary firm, discovered that boarding pass documents from multiple top airlines contain precious information that when used

together allows ill-intentioned posing as you to manage, change, or cancel your flight reservation without authentication.

Also in this case, Born criticized the bad habit to publish online the pictures of a boarding pass just to inform friends and colleagues on our next trip.

Born examined a number of boarding passes of the major airlines discovering the information they include and explaining how they can pose serious risk to the unaware holiday traveler.

Let's start comparing the boarding pass of the Delta Airlines, American Airlines and United Airlines.

Figure 2 – Delta Airlines boarding pass

Figure 3 – American Airlines boarding pass

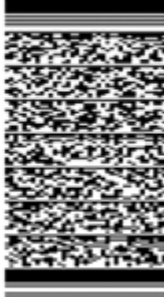*Figure 4 -United Airlines boarding pass*

Each boarding pass contains pieces of information that could be very useful for a hacker, for example, visiting the website of the Delta Airlines (**http://www.delta.com**) it is possible to verify that a user just needs the confirmation number or ticket number in order to manage, change, or cancel his flight. The same information gives the access to the traveler's first name and last name, and the remaining data present in the Delta boarding pass.

Figure 5 – Website www.delta.com 'My Trips'

The experts noticed many similarities with American Airlines and United Airlines, although United only requires users to know the confirmation number and traveler's last name, both information present of a boarding pass.
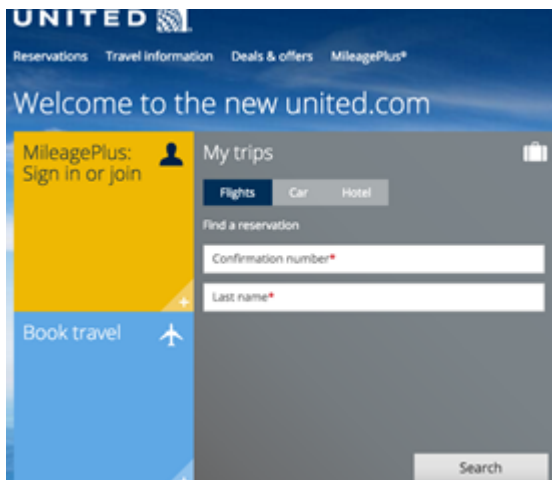

Figure 6 – United Airlines

The experts explained that on the boarding pass of the American Airlines there is the "Record Locator" an information that is similar to the confirmation number used by the other airlines he has analyzed.

Michael Born also raised many other questions about the security of the mobile boarding pass, in particular the experts warn users in connecting open Wi-Fi network and also highlighted the risk of theft of the mobile device.

Born looked at the Delta mobile app and discovered that the application stores more than just the flight information. The mobile app accesses the frequent traveler account number, user' financial data (i.e. credit card information), personally identifiable billing information and flight information.

Summarizing, don't disclose more information than necessary, especially when dealing with boarding pass. If you want to share a picture of your boarding pass online don't forget to blur the barcode if you want to avoid problems.

Most of the information contained within the barcode is harmless, but you cannot underestimate the risk of a cyber-attack. The data could be used by attackers to act in your behalf or to target you with spear-phishing emails.

I would also recommend not leaving your boarding pass on the aircraft. Unfortunately this is a common habit.

We now understand that a boarding pass is a mine of information for an attacker or a scammer. In order to reduce security risks associated with holiday travel, I suggest you to follow a few useful tips:

- Always print paper boarding pass at home, or at any other secure place.
- Don't post pictures of your boarding document online.
- In case you lose the boarding pass at the airport, notify a gate agent immediately and request a new copy of the boarding pass.
- In case you are using a mobile boarding pass instead, take care of your mobile device.
- Never use open Wi-Fi network to access the Internet, use the cellular data connection instead.
- At the end of the trip shred all boarding documents, do not leave your old boarding pass in the airplane
- Don't publish the boarding pass in social media

Enjoy your holidays and stay safe, and don't forget that criminals are always ready to take advantage of every mistake you make.

http://securityaffairs.co/wordpress/40807/digital-id/boarding-pass-personal-information.html

http://online-barcode-reader.inliteresearch.com/default.aspx

https://www.solutionary.com/resource-center/blog/2015/11/holiday-travel-security-tips/

http://www.iata.org/whatwedo/stb/documents /bcbp_implementation_guidev4_jun2009.pdf

http://krebsonsecurity.com/2015/10/whats-in-a-boarding-pass-barcode-a-lot/

https://shaun.net/posts/whats-contained-in-a-boarding-pass-barcode

http://fox42kptm.com/news/local/cyber-experts-warn-against-taking-pictures-of-your-boarding-pass