Delta Air Lines Security Center

Delta Air Lines works tirelessly to ensure the privacy and integrity of your personal information. While we are continually monitoring your SkyMiles and flight information, we recommend our customers remain vigilant by becoming aware of current fraudulent schemes and checking their online accounts. We encourage customers to report any unusual account activity to Delta Air Lines at 800-221-1212.

Fraudulent Schemes

When our consumers are aware of potential fraud scenarios, they are better able to assist Delta Air Lines in safeguarding their information and reporting instances of fraud.

SkyMiles

SkyMiles fraud occurs when an account is accessed and/or miles are deducted without account holder's consent. If you believe miles have been inaccurately deducted, or notice a change in your SkyMiles account, please change your SkyMiles password immediately, and report the incident to Delta Air Lines.

Credit Card

Credit card fraud occurs when an individual's card is lost or stolen, and then utilized for unauthorized transactions. In addition, credit card fraud can occur through the breach of an individual's credit card data (i.e. via skimming). If you have been the victim of credit card fraud, please contact the credit card company directly. If a Delta ticket was purchased as a result of credit card fraud, please report the incident to Delta Air Lines.

Phishing and Smishing

Phishing is when an individual deceives a consumer into providing personal identifying or financial information. These phishers will pose as legitimate companies, contacting you via telephone or an illegitimate email account, and persuade you to divulge confidential information; including your account passwords, social security number, or banking information. "Smishing" uses the same practices, but rather than calling your cell phone or sending you an email, you may receive a text or message on a social media account. **Delta Air Lines will never ask you for your password in an email, over the phone, or via a social media platform.**

Promotional Fraud

Often working in tandem with Phishing practices, fraudsters will use a variety of communication techniques to manipulate the customer. The following are examples of fraudulent communications not originating from Delta Air Lines:

- Emails requiring disclosure of customer information
- Postcards
- Gift Card promotional websites letters or prize notifications promising free travel
- Letters claiming you have purchased a Delta ticket, a credit card has been charged, order has been completed, or an invoice/receipt is attached to an email
- Websites offering free or heavily discounted flights for following or a liking a social media account
- ***Please note: Delta will never ask you to pay with alternative forms of payment (such as Visa gift cards, Amex gift cards, or Google Playcards).***

What You Can Do:

While Delta does everything in our power to ensure the most secure and safe means of booking your airline travel, most practical security tool for online browsing is yourself! The most powerful thing you can do in safeguarding yourself online is maintaining a keen sense of awareness, and a healthy sense of skepticism when things “don’t feel right”. When dealing online, any offer that appears to be “too good to be true” often has an individual or a group behind it that will happily take advantage of you. If you follow these steps in conjunction with keeping your wits about you, you reduce the chances of falling victim to similar issues, whether when traveling or conducting any other business online.

Remember, if a deal seems too good to be true, it probably is. If you are unsure, it is best to verify by contacting Delta Air Lines directly via the official pages and numbers located below.

Password Security

Complex and unique passwords are a crucial and safe way to prevent hackers from easily guessing your credentials and gaining access to your account. You should not use the same password across multiple websites that contain your personal information, particularly if it is used to make a purchase of any type.

Fortunately, there are utilities called “Password Managers” that make generating and securely storing passwords easier than ever. There are many types of services that offer this functionality that require minimal setup and forego the need to remember multiple passwords by auto filling and securely storing them all on their own. Password managers can be set up on both your computer and mobile device. If you are unable to configure a password manager please ensure all passwords are unique, contain at least ten characters, and use both upper, lower, special (!$&%), and number characters and do not use the same password on different websites.

SkyMiles Password:

For members of our SkyMiles program, keeping a watchful eye on your SkyMiles account can be the customer’s first indication of fraudulent activity. If you believe someone other than yourself has access your SkyMiles information, update your account password and continue to monitor your account for any misuse.

Your password on delta.com **must** contain:

- 8-20 characters
- 1 number and 1 letter
- 1 uppercase and 1 lowercase

letter Your password on delta.com **cannot**

contain:

- The "@" symbol
- Your SkyMiles number, email or username
- More than three special characters

Internet Browsing Security:

When shopping online, or visiting websites for online banking or other sensitive transactions, always make sure that the site’s address starts with “https”, rather than “http”, and has a padlock icon in the URL field. This indicates the website is secure and uses encryption to scramble your data so it can’t be intercepted by others. In addition, be on the lookout for websites that have misspellings or bad grammar in their addresses. They could be copycats of legitimate websites.

Refrain from clicking links in email messages or unofficial pages, as well as any associated attachments. Should you receive one of these messages via email, you should delete it from your inbox and disregard the website promotional claims.

Ensure you are using the latest version of your web browser. All browsers will also check for the latest version of their respective software; therefore, it can be helpful to shut down your computer completely before turning it back on for those checks and updates to occur.

The only way to be sure you are doing business with Delta Air Lines and ensure we are able to provide you with the best customer support is by going to https://www.delta.com or calling 1-800-221-1212

While many third party websites exist that may broker tickets akin to a travel agency, none of those services can offer the same insight or features our customer service can provide you. Any time you deal with a third party website claiming to represent Delta Air Lines, you risk compromising your personal information, as scammers are more frequently attempting to abuse the trust you place in us by impersonating Delta using illegitimate websites and outlets before defrauding you.

Mobile Security

Our mobile devices can be just as vulnerable to online threats as our laptops. In fact, mobile devices face new risks, such as risky apps and dangerous links sent by text message. Be careful where you click, don't respond to messages from strangers, and only download apps from official app stores after reading other users' reviews first. Make sure that your security software is enabled on your mobile, just like your computers and other devices.

Anti-Virus Software and Malware

Keep all your software updated so you have the latest security patches – this will help prevent malware from producing malicious popups on your computer. Turn on automatic updates so you don't have to think about it, and make sure that your security software is set to run regular scans.

Keep your guard up

Always be cautious about your online activity, including which sites you visit, which passwords you use, and what information you choose to share. Use comprehensive security software, and make sure to back up your data on a regular basis in case something goes wrong. By taking preventative measures, you are working with Delta Air Lines to safeguard your personal and financial information, as well as ensure a smoother travel experience.

Official Delta Air Lines Communications

Delta Air Lines: Websites and Social Media

- www.delta.com
- www.facebook.com/delta
- www.facebook.com/deltaairlinesbrasil
- www.twitter.com/delta
- www.twitter.com/deltanewsroom
- www.twitter.com/deltaajuda
- www.google.com/+delta
- www.youtube.com/DeltaAirLines
- www.pinterest.com/deltaairlines
- www.linkedin.com/company/delta-air-lines
- http://takingoff.delta.com
- Find us on Instagram @delta

Delta Air Lines: Reservations Phone Numbers

Domestic Reservation Sales
1-800-221-1212

International Reservation Sales
1-800-241-4141
1-800-800-1504

SkyMiles Representatives
1-800-323-2323

Disability Assistance
1-404-209-3434
For customers with speech disabilities, or are Deaf/Hard of Hearing: Dial 711

Customer Care
For comments or complaints regarding past travel experience: 1-800-455-2720

Your information security is vital to Delta Air Lines. If you see unusual account activity, please change your password, and contact Delta Air Lines at 800-221-1212. In addition, if you believe you have been a victim of fraud and have suffered a financial loss, you should contact your local law enforcement agency.