STOP | THINK | CONNECT™

TIPS FOR SECURING FREQUENT FLIER MILES

Recent reports have exposed a new disturbing trend for online scammers: hackers are now targeting vulnerable travelers' frequent flier miles.

As the Wall Street Journal and the Today Show report, thieves are stealing miles and points and turning them into cash, gaining access to unsuspecting fliers' accounts and trading in their hard-earned miles for cash, gifts cards, merchandise or whatever points can buy online.

With the busy holiday travel season fast approaching, these cybercriminals are undoubtedly getting ready to cash in, but with these simple steps from the National Cyber Security Alliance, consumers can fly easy knowing their miles and frequent flier accounts are safer and more secure.

DONT FORGET TO CHECK IN

Monitor your account periodically for any unusual activity, especially if you travel infrequently.

MAKE BETTER, UNIQUE PASSWORDS

A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember. Passwords for critical accounts should be unique.

ENABLE STRONGER AUTHENTICATION

Use the strongest account security available on your frequent flier accounts. Some accounts offer a backup verification option commonly known as two-step verification or multi-factor authentication. Two-step authentication, for example, requires a second step, such as a text message to a phone or the swipe of a finger to be used in addition to a password to log in to an account.

WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it. Airlines are big brands, and cybercriminals know many people have frequent flier accounts, so "phishing" tricks such as sending out email spoofing an airline will surely reach some real customers.

TRANSFER GOOD SECURITY PRACTICES

There are a lot of connections between travel accounts benefits, like miles earned or credits with other travel partners such as hotels, car rental companies and theme parks. Make sure you have unique logins, and if you feel any of those accounts have been compromised take steps to protect other accounts, such as changing your passwords.

STOP | THINK | CONNECT™

TIPS FOR SECURING FREQUENT FLIER MILES

BE SMART ON PUBLIC WI-FI

Be cautious when accessing accounts via free, unsecured Wi-Fi at airports, hotel lobbies and anywhere while traveling. Use an app or browse using your mobile connection if no secure options are available.

DONT SHARE YOUR BOARDING PASSES

Avoid sharing pictures of boarding passes on social media and dispose of them securely. Boarding passes, depending on airline, can contain a lot of private information in the barcode, such as your full name, destination, flight record number and your frequent flyer number, which in some cases is used as your account login.

KEEP LOYALTY APPS UP TO DATE

If you have installed a loyalty app, always install new updates as they become available; they often have security patches in addition to new functionality.

PROTECT YOUR MOBILE DEVICE

Having a strong passcode or using a finger wipe adds protection if your device is ever lost or stolen.