TIP SHEET SERIES **NO. 21**

Secure Your Flight Miles

According to recent reports, hackers have changed their fraud methods by taking over the flight miles. According to the Wall Street Journal and the Today Show, fraudsters are changing their cash, gift cards, or commodities for these hard-earned flight miles by taking over the accounts of innocent flying individuals. In particular, dense flight periods increase the tendency of cybercriminals to steal the flight miles. Individuals can protect their miles and flight accounts with the following suggestions.

- **Do Not Share Your Flight Cards**

  Do not share your flight card from social media and destroy it safely, when you're done. Flight cards can hold a lot of special information, such as barcode, name, surname, flight number, flight account and etc. With these information your account can be stolen. Also, If you often travel, periodically monitor your account to see any unusual activity.

- **Create Unique and Strong Passwords.**

  A strong password must contain at least 12 characters. Strong passwords should be created by focusing on proverbs, favorable positive sentences, idioms to create a password.

- **You should create different passwords for different accounts**

  If you feel any threat to your accounts, you should immediately change your passwords.

- **Enable Identity Authentication**

  Enable all security options in your flight account. Two-step authentication should be used for existing accounts. Two-step authentication can use everything from a short message to a phone to a biometric icon, such as a fingerprint, to provide enhanced account security.

- **Delete If You Suspect Anything**

  Cybercriminals often swipe personal information via links in email, social media messages, or online advertisements. Even if the source is known, it should be deleted immediately when something seems suspicious.

- **Be Careful About Public Wi-Fi**

  Public Wi-Fi is not secure. Any attacker can see what you can do while connected to this network. In such environments, limit business types that contain sensitive information such as credit card, password, customer data. If no security option is available, use your mobile connection with an application or browser.

- **Keep Applications Updated**

  Keep your applications up-to-date. Because the security patches of current applications have been established.