October 23, 2019
bitFlyer, Inc.

Caution: Phishing Sites Are Placing Ads in Search Results on Search Engines Such as Google

We have confirmed that there are phishing sites that are placing advertisements in the search results for Google or other search engines in order to impersonate bitFlyer.

1. What is phishing?

Phishing refers to when someone sends an email that impersonates a real company that leads to a phishing website with the intent to steal personal information. If someone's email address and password are stolen through a phishing site, the customer faces a risk of having their assets stolen through unauthorized access.

Do not enter your email address, password, or other information on a phishing site. If you have entered your email address, password, or other information on a phishing site, please change your email address and password immediately.

2. Ways to avoid being phished

Please take the following points into consideration to help avoid being phished.

- Before clicking the URL, ensure that it begins with https://bitflyer.com. A phishing site may change a letter to resemble the correct URL. For example, replacing the "e" with an "o."
- Access our website through a bookmark rather than through a link in a suspicious email or on an online message board.
- If you receive an email from a sender using bitFlyer's name that directs you to an abnormal login procedure, do not follow its instructions.
- Consider enabling two-factor authentication as a way to protect yourself in case you accidentally enter your email or password into a fraudulent website.
- Confirm the site's certification. More information on how to confirm certification can be found here.

For more information on Phishing, please thoroughly read and understand Beware of fraud in the form of phishing on our website.