Subject: **Advisory – Prevention Against https Based Phishing Attacks (Advisory No. 10)**

1. **Introduction.** Phishing attacks are increasing at a rapid scale as hackers are increasingly utilizing **third party https-based services** to host fake credential harvesting pages. **Most of antimalware solutions don't detect https:// based phishing pages** and **it becomes the responsibility of the user** to be well aware of these techniques.

2. **Technical Details.** Attackers utilize various techniques for phishing purposes, a general methodology of attack is listed below: -

a. Attackers host legitimate looking web pages of banking and email websites on authentic web hosting cloud services like **000webhostapp.com, heroku.com** etc to avoid anti malware detection.

b. These legitimate looking URLs are send to the user with convincing content via spoofed emails.

c. Upon clicking on the link, the victim is redirected to the hacker's website where he can trick the user by entering the login credentials.

3. **Recommendations.** Following safeguards are recommended to secure from **https:// based phishing attacks: -**

a. Always make sure that the page on which credentials are being **entered has correct characters and a legitimate URL** with **https://** tag, e-g:-

Ser	Legitimate URL	Illegitimate URL
(1)	https://www.facebook.com	https://www.faceb00k.com
(2)	https://login.yahoo.com	https://data-mail-yahoomail-email.com
(3)	https://www.gmail.com	https://sites.google.com
(4)	https://www.twitter.com	https://twi11er.com

b. It is mandatory to utilize **2 - factor authentication** on all email and banking accounts.

c. Keep **browser and operating system** along with all software **up to date**.

d. Install and update well reputed anti-malware solution like Kaspersky, AVAST, Avira etc.

e. To **prevent from the threat of clicking on random popups** and **advertisements**, it is advised to utilize **Adblock** or **Adblock** plus extensions.
f. Make sure that both **host - based firewall** and **network - based firewall** are active and employed in your network.