Annexure-B

ADVISORY: PHISHING ATTACK

Phishing domains are malicious websites designed to trick users into divulging sensitive information, such as login credentials, financial information, or personal data.

Identifying Phishing Domains

To avoid falling victim to phishing domains:

1. **Be cautious of unsolicited emails or messages:** Legitimate organizations rarely ask for sensitive information via email or message.
2. **Verify the domain name:** Check the URL carefully, looking for misspellings, extra characters, or variations in the domain name.
3. **Watch for poor grammar and spelling**: Legitimate websites usually have professional content.
4. **Be wary of urgent or threatening messages**: Phishing domains often try to create a sense of urgency to prompt users into taking action.
5. **Check for HTTPS and a valid SSL certificate:** Legitimate websites usually have a valid SSL Certificate and use HTTPS.

To protect from phishing domains:

1. **Use strong, unique passwords**: Avoid using the same password across multiple sites.
2. **Enable two-factor authentication (2FA):** 2FA adds an extra layer of security to prevent unauthorized access.
3. **Keep your software and operating system up to date:** Ensure you have the latest security patches and updates.
4. **Use anti-virus software and a firewall:** Protect your device from malware and unauthorized access.
5. **Use a reputable password manager:** Consider using a password manager to securely store and generate strong passwords.

Reporting Phishing Domains

If suspected phishing domain:

1. **Do not interact with the website:** Avoid clicking on any suspicious links or providing any sensitive information.
2. **Report the website to the relevant authorities:** Inform your organization's IT department or report the phishing email to Cyber and Information Security Management Division (NIC).
3. **Delete any suspicious emails or messages:** Remove any emails or messages related to the phishing domain.