Phishing Mail Advisory

Do’s

1. **Be cautious and sceptical**: Always approach emails with caution, especially those from unknown or suspicious sources.

2. **Verify the sender**: Check the sender's email address and ensure it matches the official contact information of the organization they claim to represent.

3. **Check for spelling and grammar errors**: Phishing emails often contain typos, grammatical mistakes, or awkward language.

4. **Hover before you click**: Hover your mouse over any links in the email to reveal the actual URL. Ensure the URL matches the one displayed in the email and is not a deceptive link.

5. **Keep software up to date**: Regularly update your email client, web browser, and operating system to protect against known vulnerabilities.

6. **Use strong, unique passwords**: Create strong passwords and use a password manager to securely store them.

7. **Enable two-factor authentication (2FA)**: Enable 2FA whenever possible to provide an extra layer of security for your email account.

8. **Educate yourself**: Stay informed about the latest phishing techniques and scams to better recognize and avoid them.

Don’ts

1. **Don't click on suspicious links**: Avoid clicking on links in emails unless you are confident about their authenticity.

2. **Don't download attachments from unknown sources**: Be cautious when downloading attachments, especially if they are unexpected or from unfamiliar senders.

3. **Don't provide personal information**: Legitimate organizations would never ask for personal or financial information via email. Avoid sharing sensitive data like passwords, credit card details, or social security numbers through email.

4. **Don't trust urgent or threatening messages**: Phishing emails often use urgent or threatening language to manipulate victims. Be sceptical of such messages and verify their legitimacy through other means.

Cyber Hygiene Steps

1. **Use robust email filters**: Enable strong spam filters and configure them to mark or divert suspicious emails to the spam folder.

2. **Install antivirus and anti-malware software**: Keep your computer protected with up-to-date security software to detect and block phishing attempts.

3. **Regularly back up your data**: Create regular backups of important files and data to mitigate the impact of any potential phishing attacks.

4. **Report phishing attempts**: If you receive a phishing email, report it to your email provider and relevant authorities so that appropriate action can be taken.

5. **Stay updated on security best practices**: Continuously educate yourself about cybersecurity best practices and follow the latest recommendations to enhance your online security.