SAC Website Notice on Phishing Emails

SAC has been notified of fraudulent cases involving the issuance of fake SAC invoices requesting payment to a 3rd-party company. These phishing emails aim to trick any unsuspecting users into clicking on the given link to make payment to their accounts.

Please refer to the SUNDAE Principle below to identify such emails:

|  |
| --- |
| **SUNDAE Principle** |
| **S**pelling errors and bad grammar |
| **U**rgent or threatening message |
| **N**ame of sender does not match email address |
| **D**omain Name or email address does not appear legitimate |
| **A**ttachment looks malicious |
| **E**mail containing links with misleading addresses |

If you receive emails that look suspicious:

* **DO NOT CLICK** on any link(s) in the email body.
* **DO NOT OPEN** any attachment(s) in the email.
* **REPORT** any suspicious email received by leveraging the **Report Phishing** in your Microsoft Outlook or feedback functions in other email platforms/software.
* **DELETE** all spam email(s).

Please be cautious not to click on suspicious **hyperlinks**, open suspicious **attachments** or make any payments to third party entities without first verifying the authenticity and legitimacy of the email received.

Should you need further clarifications, please email [sac@enterprisesg.gov.sg](mailto:sac@enterprisesg.gov.sg).