How to identify a fake email, SMS or website

Asking you for sensitive information

Fake emails claim that your information has been compromised and/or your account de-activated or suspended, and hence asking you to confirm the authenticity of your information and/or transactions.

Appearing to be from a legitimate source

While some emails are easy to identify as fraudulent, others may appear to be from a legitimate source. However, you should not rely on the name or address in the 'From' field alone as this can be easily duplicated.

Containing spelling mistakes

Very often such 'phishing' mails may contain several spelling mistakes. Even the links to the counterfeit websites may contain a URL with spelling mistakes to take you to a website which looks like that of your bank – but is not. Whenever you use a link to access a website, be sure to check the URL of the website and compare it with the original. It is recommended that you type the URL yourself whenever you access a bank, or you may bookmark or store the URL in your 'list of favourites'.

Containing prizes or other offers

Some fake emails promise a prize or gift certificate in exchange for completing a survey or answering a few questions – to collect the alleged prize, you may be asked to provide your personal information.

Containing fraudulent job offers

Some fake emails appear to be sent by companies to offer you a job. These are often work-at-home positions which are schemes that victimise both the job applicant and other customers. Be sure to confirm that the job offer is from a genuine and reputed company before responding.

Linking to counterfeit websites

Fake emails may direct you to counterfeit websites carefully designed to look real. Such websites may look very similar and familiar to you but are used to collect personal information for illegal use.