Ministry of Health

# E-MAIL PHISHING & SMISHING

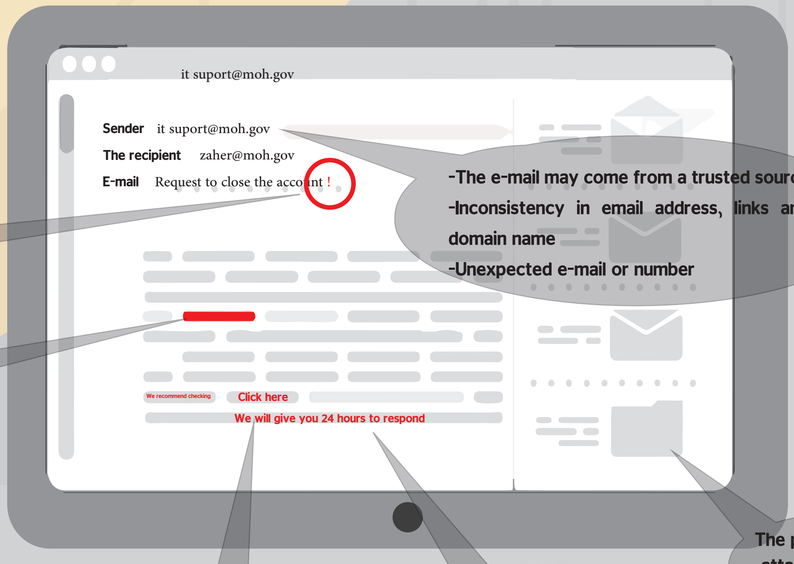
Be ware of malicious e-mails that may impersonate a trusted user or a specific organization.

Be aware of SMS messages, social media messages, or WhatsApp messages that ask you to update your data, change your password, or warn of an account being hacked, or clicking on an electronic link.

## Check for phishing signs availability

- The presence of an electronic link.
- There are spelling and grammatical mistakes.
- Unexpected e-mail or number.
- A suspicious sense of urgency/an urgent request for a response.
- Use general greetings/unfamiliar greetings.
- The presence of attachments in the e-mail.
- Unusual request/request for personal information.
- Inconsistency in email address, links and domain name.
- The e-mail may come from a trusted source.
- Offers for unexpected prizes or rewards.
- A request for money.
- There is a red mark in the e-mail.

## Awareness template for email phishing




There is a red mark in the e-mail

There are spelling and grammatical mistakes

-The e-mail may come from a trusted source
-Inconsistency in email address, links and domain name
-Unexpected e-mail or number

Inconsistency in email address, links and domain name

A suspicious sense of urgency/an urgent request for a response

The presence of attachments in the e-mail

◇ Not all signs are required