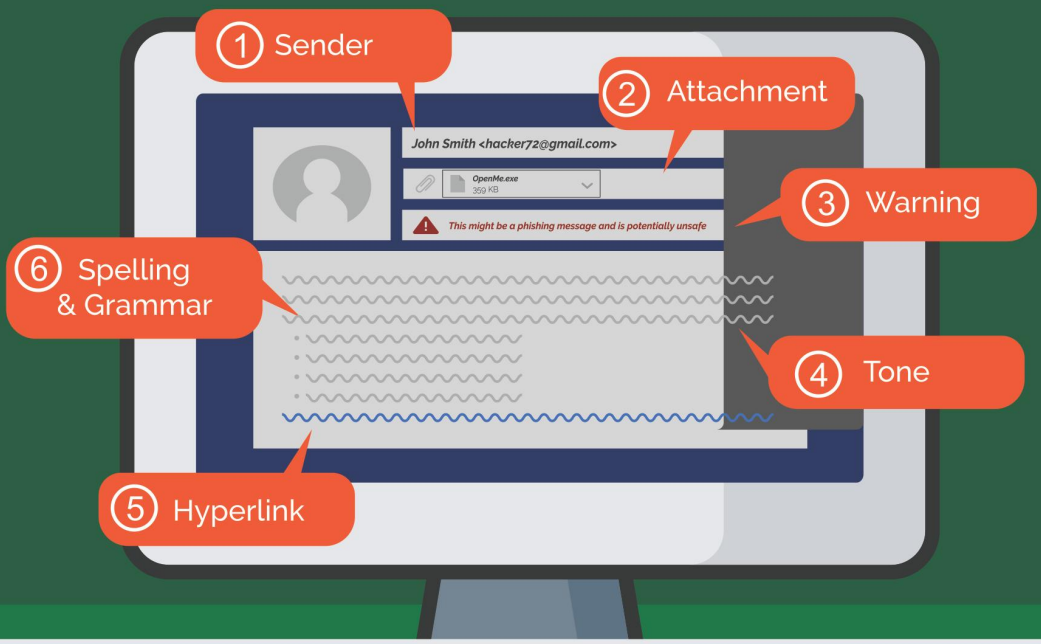
# CYBER SECURITY AWARENESS

## How to Spot a Phishing Email




| | | |
|---|---|---|
| 1 | Sender | Always check who the sender is when you receive an email. You should be on alert if you don't recognize the sender, the display name doesn't match the email address, or if the email address is from a suspicious domain. |
| 2 | Attachment | Do not click on an attachment if you don't recognize the sender or if the attachment is nonsensical or unexpected. File types can be masked so do not assume any file type is completely safe. When in doubt, report it to your IT department. |
| 3 | Warning | If you have phishing warning enabled on your email platform, any email that is a potential threat will be flagged. It is possible that some phishing emails won't get flagged by the auto-detection so exercise caution while dealing with every email. |
| 4 | Tone | Phishing emails often give off a tone or urgency or danger. An urgent tone will cause some users to take action immediately without thinking it through. An example of using an urgent tone would be an email telling you an account of yours has been compromised and you need to click this link to recover your account. |
| 5 | Hyperlink | Always inspect links thoroughly before clicking on them. Check to see if the link is a misspelling of a common website. Links can be spoofed so use your mouse to hover over a link and make sure the pop-up link is consistent with the link in the email. |
| 6 | Spelling & Grammar | Spelling and grammatical errors are common in phishing emails. If an email is riddled with spelling and grammatical errors then that should tip you off that the email may not be legitimate. |


the dpsa
Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

Powered by SITA
stateinformationtechnologyagency

# CYBER SECURITY AWARENESS

# Don't Get Hooked

## 6 Tips to Avoid Phishing Attacks

### 1 Watch out for Emails That Have Improper Grammar or Spelling

One of the most common signs that an email isn't legitimate is that it contains spelling and grammar mistakes. Check the email closely for misspellings and improper grammar.

### 2 Check That Hyperlinked URLs are the Same as the URL Shown

The hypertext link in a phishing email may include the name of a legitimate organization. However, when you move the mouse over the link (without clicking it), the actual URL is different than the one displayed.

### 3 Be Wary of Emails That Urge You to Take Immediate Action

Phishing emails often try to trick you into clicking a link by claiming that your account has been closed or put on hold. Don't click the link no matter how authentic it appears. Login to the account in question by directly visiting the appropriate website, then check your account status.

### 4 The Email Claims You've Won a Contest You Haven't Entered

If you receive an email notifying you that you won the lottery or another prize when you haven't entered a contest, the email is probably scam. Don't click the link or give any personal information.

### 5 The Email Asks You to Donate to a Worthy Cause After a Tragedy

Scammers often send phishing emails inviting people to donate to an organization after a natural disaster or other tragedy. The links send users to malicious sites that steal credit card and other personal information. If you'd like to make a donation to charity, visit the website directly.

### 6 Suspicious Attachments Sent via Email Should Never be Downloaded

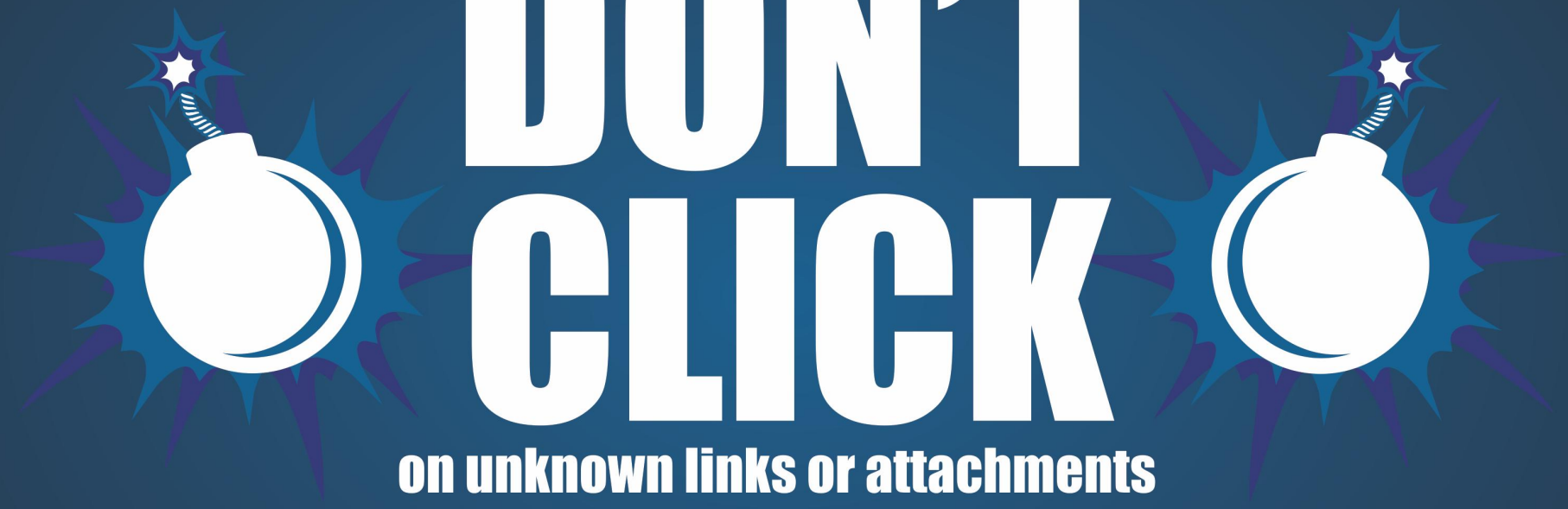
Typically, you shouldn't receive an email with an attachment unless you've requested the document. If you receive an email that looks suspicious, **DON'T CLICK** to download the attachment.


the dpsa
Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA


**Information security is everybody's responsibility!**


Powered by SITA
stateinformationtechnologyagency

# CYBER SECURITY AWARENESS




- Be cautious of unsolicited emails and those requesting personal information.
- Be suspicious of emails that look unprofessional.
- Verify the sender's email address.
- Hover over the link to verify its destination.
- **NEVER** click on unknown links or attachments.
- For any suspicious email Contact SITA Help Desk **012 672 1818** or Email to **sitasc@sita.co.za**.

the dpsa
Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

Powered by SITA
stateinformationtechnologyagency