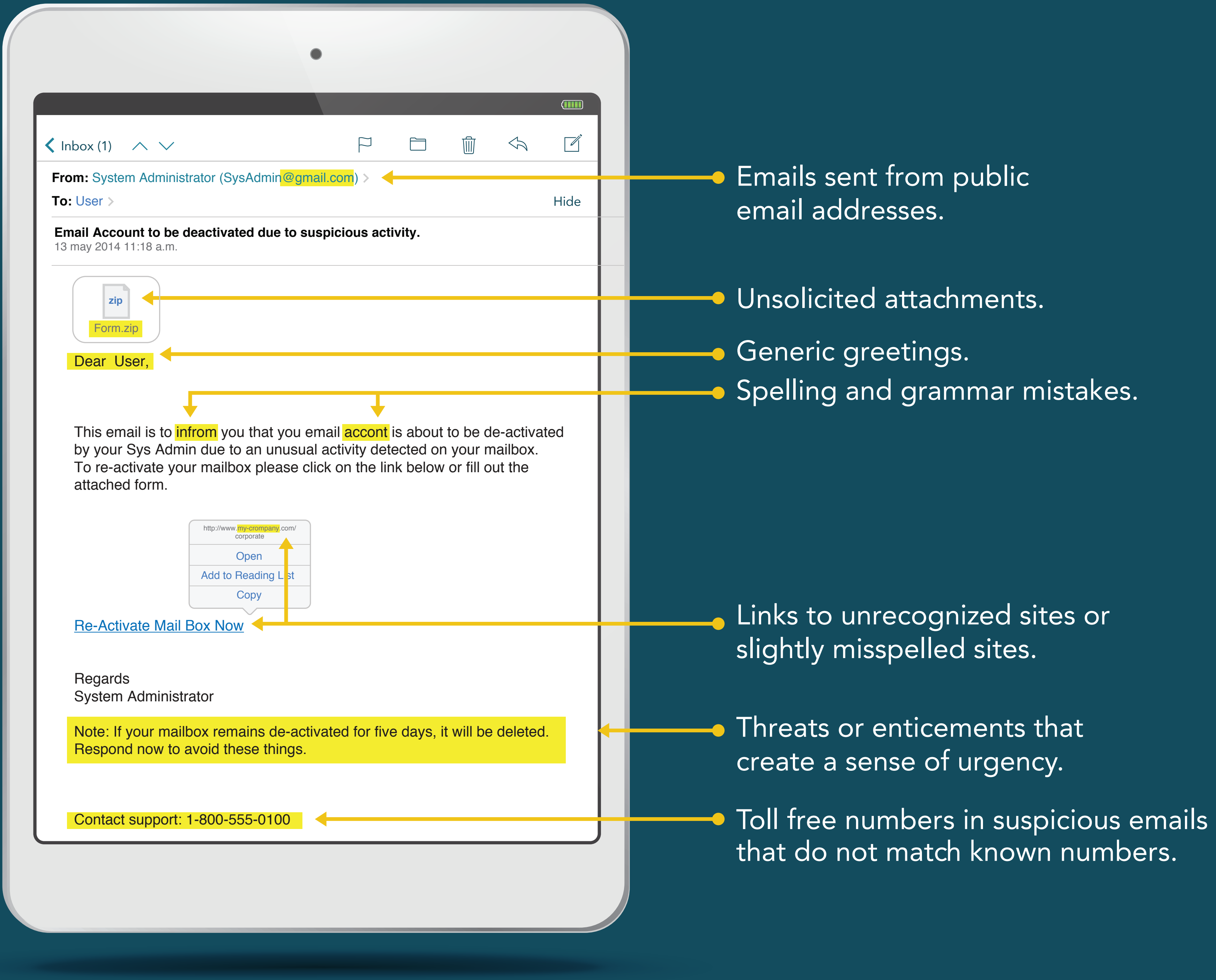
HOW TO DETECT A PHISHING EMAIL



From: System Administrator (SysAdmin@gmail.com)

To: User

Email Account to be deactivated due to suspicious activity.
13 may 2014 11:18 a.m.

zip
Form.zip

Dear User,

This email is to infrom you that you email accont is about to be de-activated by your Sys Admin due to an unusual activity detected on your mailbox. To re-activate your mailbox please click on the link below or fill out the attached form.

http://www.my-crompany.com/corporate

Re-Activate Mail Box Now

Regards
System Administrator

Note: If your mailbox remains de-activated for five days, it will be deleted. Respond now to avoid these things.

Contact support: 1-800-555-0100

- Emails sent from public email addresses.
- Unsolicited attachments.
- Generic greetings.
- Spelling and grammar mistakes.
- Links to unrecognized sites or slightly misspelled sites.
- Threats or enticements that create a sense of urgency.
- Toll free numbers in suspicious emails that do not match known numbers.

What to Do:

1. Never give out personal or sensitive information based on an email request.
2. Don’t trust links or attachments in unsolicited emails.
3. Hover over links in email messages to verify a link’s actual destination, even if the link comes from a trusted source.
4. Type in website addresses, rather than using links from unsolicited emails.

inspired eLearning®
education for your enterprise

InspiredeLearning.com