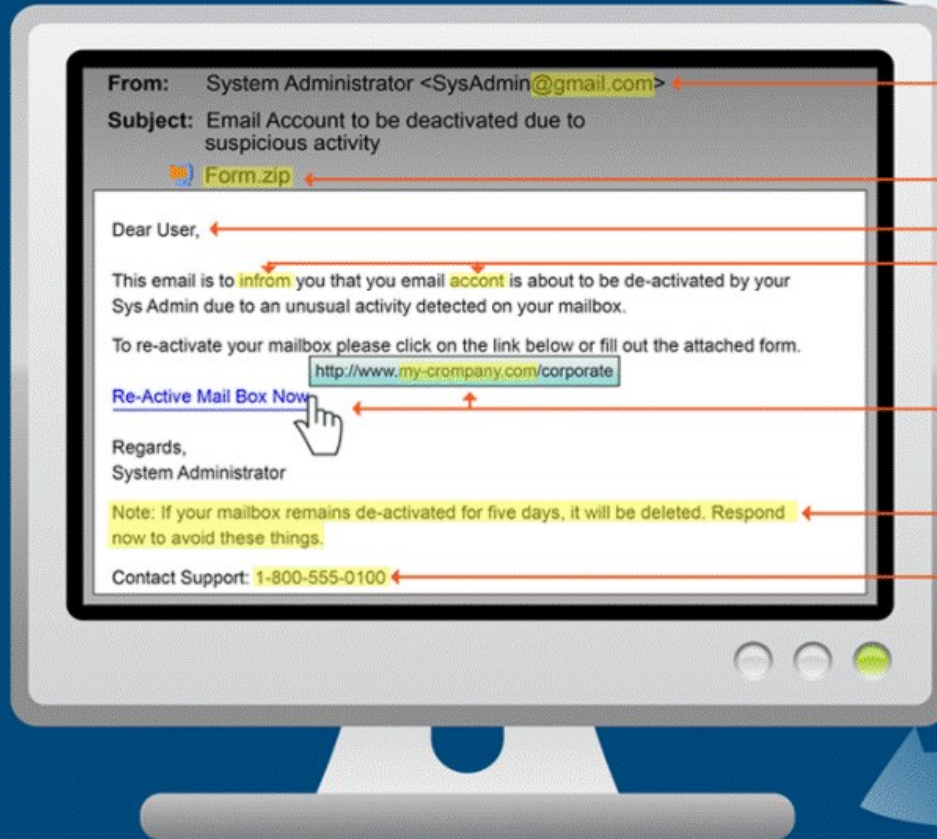# You've Been Phished...

We are testing the security awareness of employees by sending out simulated phishing emails. If you are seeing this page, you must have clicked on a link in one of them.

How to Detect a Phishing Email

From: System Administrator <SysAdmin@gmail.com>

Subject: Email Account to be deactivated due to suspicious activity

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-Active 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

1. Email sent from public email addresses

2. Unsolicited attachments

3. Generic greetings

4. Spelling and grammar mistakes

5. Links to unrecognized sites or slightly misspelled sites

6. Threats or enticements that create a sense of urgency

7. 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.

5. If an email from a friend or colleague seems suspicious, call them and ask if the email is legitimate.

6. Be suspicious of phone numbers in emails. Use the phone number found on your card or statement or in a trusted directory instead.

Notes

- This assessment is part of a training program meant to help sensitize you to phishing emails and help you avoid falling for the real thing.

- Phishing test results are not reported to supervisors or management, except in extreme cases of users repeatedly and consistently falling for simulated phishing emails.

What Is Phishing?

Phishers typically create fake emails that appear to come from someone you trust, such as a bank, credit card company, or a popular website. These emails typically try to trick you into giving away sensitive information, such as your username, password, or credit card details.

They may also try to get you to inadvertently install malicious programs on your computer, which can happen when you click on an infected link or open an infected attachment. Once the computer is infected, the phisher can monitor all of your activity, including all of your keystrokes.