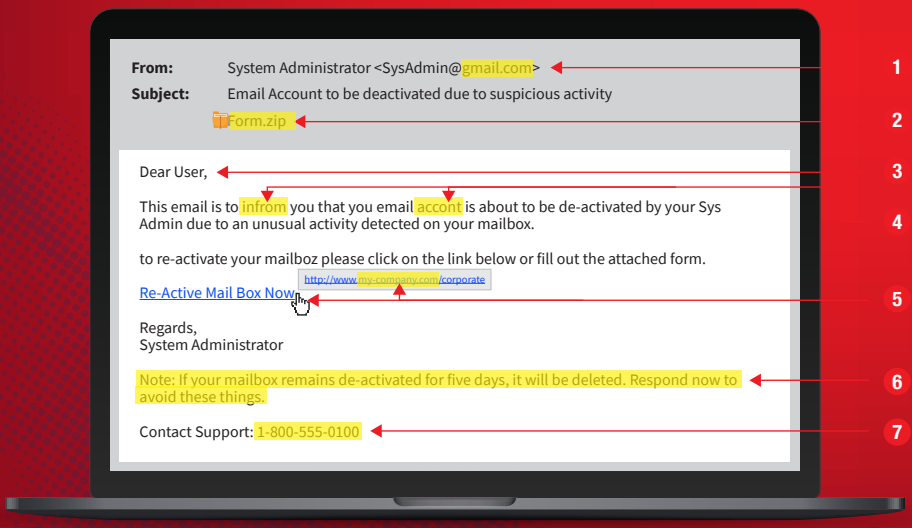
How to Detect a Phishing Email

Around 500 million phishing emails are sent per day and they are effective. Every 60 seconds, 250 computers are hacked. These breaches cost companies $388 Billion a year in stolen business secrets and intellectual property.

Here is what to look for to avoid getting phished.

The Anatomy of a Phishing Email



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

Phishing By The Numbers

91% of cyber-attacks begin with a spear phishing email

94% of spear phishing emails use malicious file attachments

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 infected, the phisher can monitor all of your activity, including all of your keystrokes.

BACS CONSULTING GROUP

(650) 747-8370