

# 7 Signs of Phishing

Can you spot a phishing attack?



## 1. Who Is This “From?”

Watch out for emails that appear to come from official organizations, such as your bank, but the From or Reply-To address is actually someone’s personal email account, such as @gmail.com.

## 2. An URGENT Subject

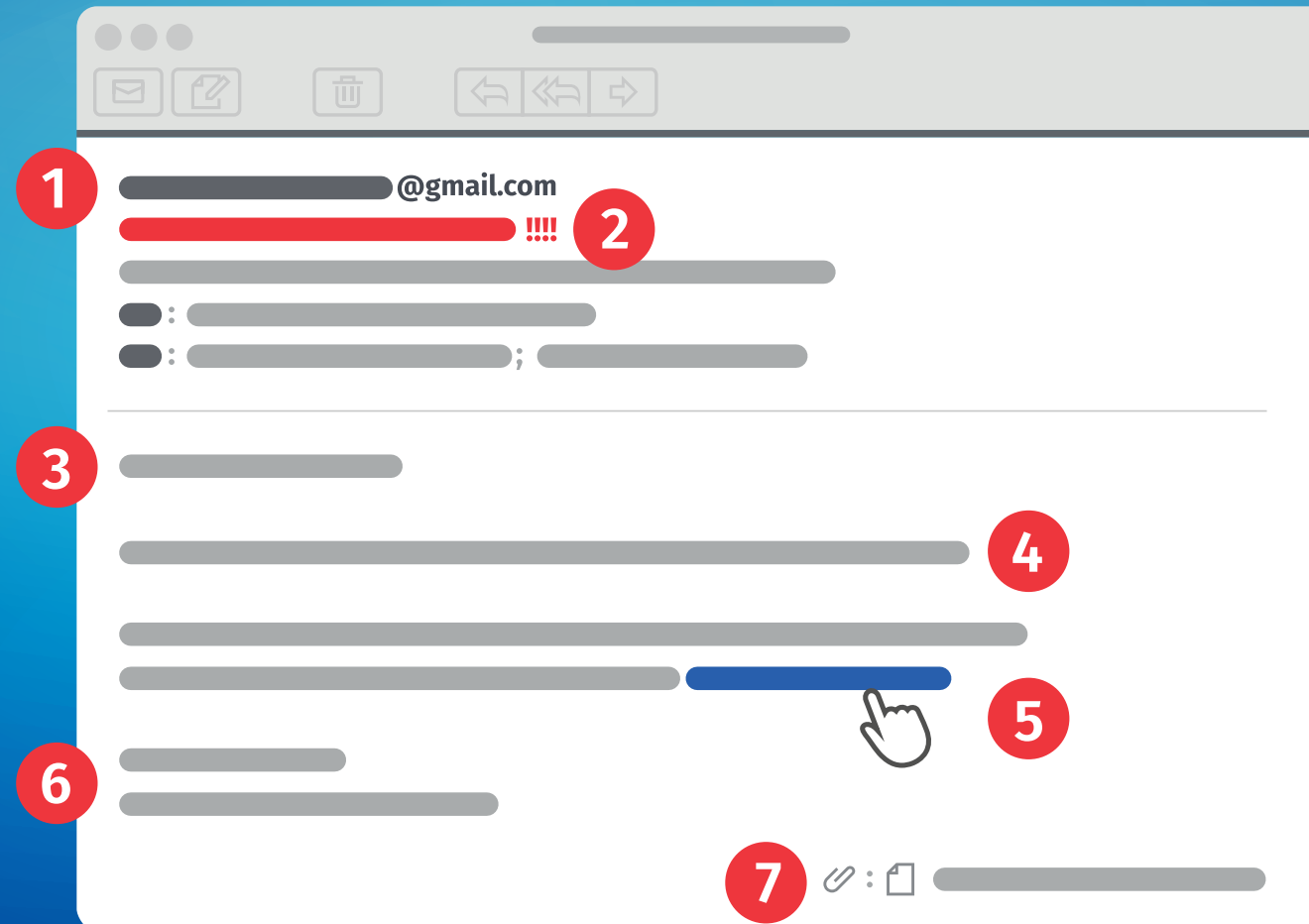
Does the subject line try to create a tremendous sense of urgency or curiosity?

## 3. Generic Greetings

Watch out for generic solutions or greetings, such as “Dear Customer.”

## 4. “I just need your credit card number...”

Is the sender asking for your password, bank account details, or some other sensitive data?



## 5. Check Before You Click

Hover over links to find the true destination before clicking on them. If a link redirects you to an unexpected location, do not click on it.

## 6. Suspicious Characters

Be on the alert if an email comes from a friend or co-worker, but seems odd or doesn’t read like something they would send.

## 7. Don’t Get Attached

Do not open unexpected or suspicious attachments.

**Stay Alert.**  **Phish Happens.**