How to Spot a Phishing Email

**Generic subject line**
Legitimate emails usually have detailed subject lines. A vague subject line can be a key indicator of a phishing scam.

**Suspicious URL**
Hover over links included in emails to see the actual destination of the URL.

**Improper use of copyright**
Watch for improper use of copyright information. This is used to make the phishing email look official.

**From: Webmail Master Security (webmastersecurity@webmail.com)**

**Subject: Urgent Email**

**Dear Webmail User,**

You are required to authenticate your account below to continue sending and receive messages. We strongly advise you to upgrade now to protect your web/Domain and avoid termination. Follow link to verify your email address immediately.

www.security.webmail.com

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

**Wondering why you go this email?**

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master

©2017 Webmail Domain

**Learn more at security.ucop.edu**

**Bad grammar/spelling**
Phishing emails often contain misspelled words and bad grammar. This is a sign that the email did not come from a professional organization or a real person you may know.

**Unnecessary urgency**
Use your intuition and if something “feels” wrong, consider calling the organization or office directly to validate the email.