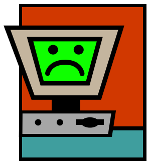
THINK BEFORE YOU CLICK!



Be cautious about all communications. Use common sense when communicating with users you do and do not know. Do not open email or related attachments from un-trusted sources.

Do not click on URLs in emails from unknown sources. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.

OCFS Information Security Unit – 03/11