

(Continued)

- ▶ May include maliciously-crafted attachments with varying file extension or links to a malicious website
- ▶ May appear to be from a position of authority or legitimate company:
 - Your employer
 - Bank or credit card company
 - Online payment provider
 - Government organization
- ▶ Asks you to update or validate information or click on a link
- ▶ Threatens dire consequence or promises reward
- ▶ Appears to direct you to a web site that looks real

Spear phishing specifically:

- ▶ Has a high level of targeting sophistication and appears to come from an associate, client, or acquaintance
- ▶ May be contextually relevant to your job
- ▶ May appear to originate from someone in your email address book
- ▶ May contain graphics that make the email look legitimate