Responses to Suspicious Activities

- Unsolicited and recurring, persistent contact
- Repeated "chance encounters"
- Unexpected system reboots or odd application behavior
- Impossible or failed logins or unusual account lockouts
- Suspicious or unexpected email settings or configurations
- Unauthorized system access or disclosure of information
- Suspicious IP addresses and/or foreign URL endings
- Emails from supposed persons of authority or legitimate companies
- Emails containing poor grammar, misspellings, and/or generic greetings

- Quickly developed personal relationships or associations
- Offers of payment for travel expenses
- Third party insert into an existing two-way official or social relationship
- Use of recording devices without approval or unusual absences (to record notes)
- Attempts to obtain biographic information about yourself or others or inappropriate interest in or observation of you
- Odd feeling you keep bumping into same person or seeing them in various places
- Person knows more about you than you do about them
- Extravagant “wining and dining” or other special treatment
- Unauthorized data storage or transmission
- Unauthorized hardware and software modifications
- Malicious attachments with links to a website that appear legitimate

- Encouragement of minor violations of laws or rules
- Displays of or encouragement to disregard institutional policies
- Sense that someone keeps glancing at your screen or documents
- New or increased abnormalities of smart devices’ functions after travel
- Offers of money, prestige, or privileged accesses (to equipment, labs, or information) and other “gifts”
- Appearance at locations (e.g., conferences, lectures, etc.) incompatible with area of expertise or professional occupation
- Requests for updates or validation of personal information
- Last minute changes in plans to or introduction of unknown persons or parties
- Just seems too good to be true…or just not right

- Offers of inappropriate or surprising sexual companionship, money, resources
- Mentions of or direct requests for sensitive information
- Possession of information that could be used as blackmail
- Use of ransomware or other cyberattack that demands specific response
- Threats of dire consequence or promises of great reward for you or loved ones

Created by Laura Provencher (University of Arizona) and Jessica Graham (Vanderbilt University).