Mission Assurance for Senior Leaders:
Whaling

Be vigilant, not a victim.
Protect yourself. Protect the mission.

Identifying the Threat

Whaling is form of phishing sent to senior executives or other high-level officials due to their high profile and their potential access to sensitive and classified information. Whaling may also target the senior leader's family.

Falling victim to a whaling attack provides hackers with an easy path to organizational systems or other people with inside information.

Whaling Goals

- Trick you into revealing personal or sensitive information
- Attempt to gain access to a computer or network by requesting that you click a link to download a document or visit a website in order to:
    - Install malware
    - Steal sensitive information
    - Disable networks

Signs of Whaling

- Appears to come from inside organization or legitimate outside source
- Contains specific details involving the senior leader's role
- References urgent or high interest matter
- Possibly sidesteps normal protocols
- Appears to be from someone the senior leader knows
- Contains personal information

Why Whaling is Convincing

- Spoof e-mail addresses so they appear to be real
- Research senior leader's role and personal life through:
    - Organizational websites
    - Social media and networking accounts

How to Protect Against Whaling

- Be wary of e-mails asking for personal or sensitive information
- Don't click on unexpected attachments or unconfirmed URLs
- Be careful about the information you post about yourself online
- Be suspicious of urgent e-mails about topical issues
- Verify the sender's identity
- Make sure your staff knows what to look for
- Report whaling attempts to your Security POC

You are a target. Don't be a victim. Protect your mission.