AOS
Expect the Best!

AOS Security

Social engineering is evolving so rapidly that technology solutions, security policies, and operational procedures alone cannot protect critical resources. Even with these safeguards, hackers commonly manipulate employees into compromising corporate security. Victims might unknowingly reveal the sensitive information needed to bypass network security, or even unlock workplace doors for strangers without identification. While attacks on human judgment are immune to even the best network defense systems, companies can mitigate the risk of social engineering with an active security culture that evolves as the threat landscape changes.

AOS helps organization create awareness plans to combat the social engineering vector of cybersecurity. From including passive reconnaissance with our vulnerability assessments to delivering educational content around security for organizations. AOS can help you develop a Security Culture inside your organization.

What can I do to protect myself from social engineering?

- Always trust but
  - Network Documentation
  - Secure Network Design
  - Current Refresh Cycle
- Physical Security
  - Access Controls
  - Security Cameras and Video Surveillance
- Compliance
  - Risk Management
  - Business Continuity
  - Vendor Management
- Configuration and Change Management
  - OS Deployment
  - User Provisioning
  - Virtualization
  - Backup Strategy
  - Asset Management
  - Cloud Strategy