**Risk Analysis Report: AI/ML Tool for Phishing Domain Detection**

**Technical Risks:**

* Model Performance:
  + - Challenges in accurately identifying phishing domains
    - Potential overfitting to training data
    - Variations in performance across different types of phishing attacks
    - Data Quality Issues
  + Biased or insufficient training data hindering effective generalization to new or unseen phishing domain patterns
* **Operational Risks:**
  + Scalability Issues:
    - Inefficiency in processing large volumes of domain data in real-time
    - Resource constraints impacting performance
  + Model Interpretability Challenges:
    - Lack of transparency in decision-making process
    - Limited ability to provide explanations to users
* **Security Risks:**
  + Adversarial Attacks:
    - Manipulation of inputs compromising model integrity
    - Generation of sophisticated phishing domains evading detection
  + Privacy Concerns:
    - Unauthorized access or misuse of user data
    - Potential breaches of confidentiality undermining user trust
* **Compliance Risks:**
  + Non-Compliance with Data Protection Regulations:
    - GDPR or CCPA violations due to privacy concerns
    - Legal liabilities and financial penalties
  + Failure to Comply with Industry Standards:
    - Regulatory scrutiny and enforcement actions
    - Risks to organizational reputation and trustworthiness