**Phishing Attack Scenario Analysis**

**Phishing Website Used: *altsecureservice.univer.se***

Phishing attacks are designed to deceive users into providing sensitive information such as login credentials and personal data. The analysis of the phishing scenario based on the scanned website highlights several red flags that indicate malicious intent.

**Key Indicators of Compromise:**

1. ***Suspicious URL Structure:*** The domain name (altsecureservice.univer.se) attempts to mimic a legitimate security service, which is a common technique used by attackers to mislead users.
2. ***Lack of HTTPS Encryption:*** The absence of SSL/TLS encryption (HTTPS) means the website does not secure user data transmission, making it susceptible to Man-in-the-Middle (MITM) attacks.
3. ***Fake Login Page:*** The scanned phishing site presents a login page that closely resembles a legitimate website. This tactic is used to harvest login credentials from unsuspecting users.
4. ***Missing Security Headers:***
   * No **Content Security Policy (CSP):** Without a CSP, attackers can execute malicious scripts within the website.
   * No **X-Frame-Options:** This makes the site vulnerable to Clickjacking attacks.
   * No **HTTP Strict Transport Security (HSTS):** This allows attackers to force users onto an unencrypted version of the site, increasing risks of data interception.
5. ***Social Engineering Tactics:***
   * The phishing site may display urgent messages, such as "Your account has been compromised" or "Verify your details now!" to create panic and rush users into entering their credentials.
   * Emails directing users to the site often contain grammatical errors, misleading sender addresses, or overly urgent language.

