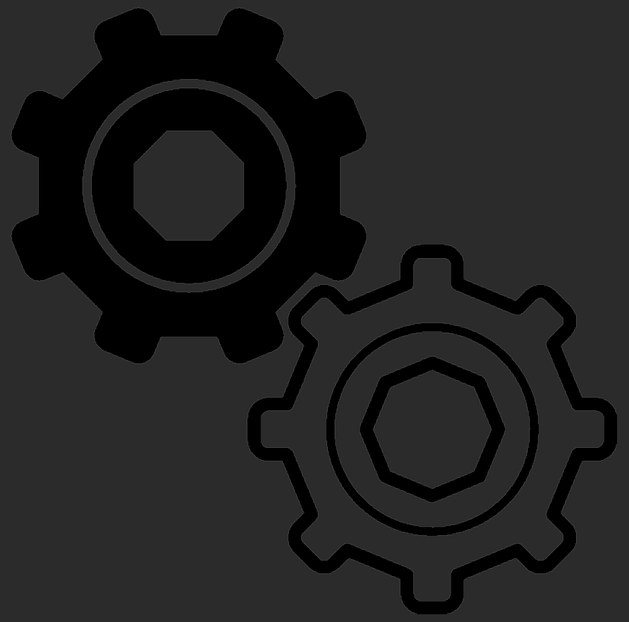
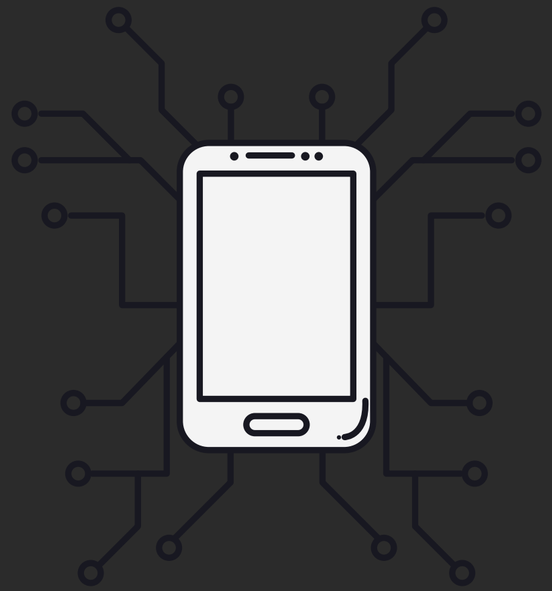
What is phishing?

Phishing es a widespread and persistent cybersecurity threat where attackers trick users into disclosing sensitive information like passwords or financial data through fraudulent messages.

Informatiion resource affected

- User credentials, personal and financial information
- Corporate systems, email accounts, and social media profiles

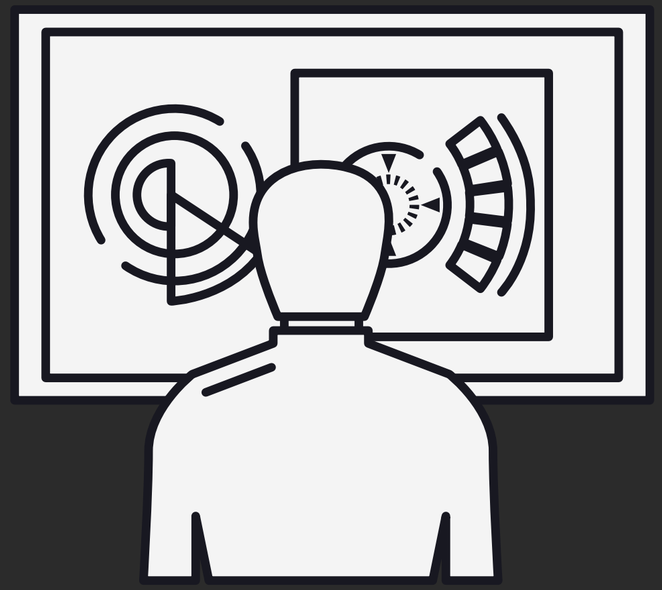




Modus operandi

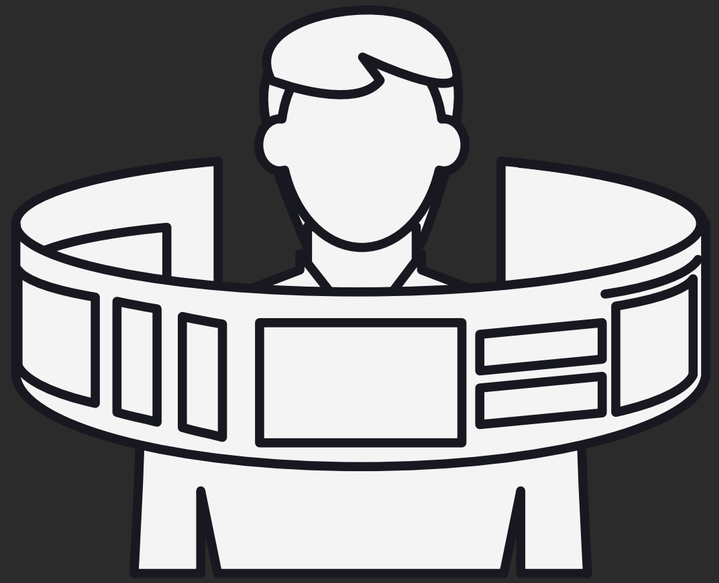
- Attackers send emails, text messages, or malicious links impersonating trusted entities (e.g. banks, companies, or online services)
- The employ social enginnering tactics, such as creating a sense of urgency or fear, to manipulate victims into clicking links or sharing confidential information

Threat Actors



- Cybercriminals seeking financial gain
- State sponsored groups for espionage or surveillance purposes
- Hacktivists targeting individuals or organizations to steal data or spread ideological messages.

Protection Measures



- Awareness and Training. Educate users or identifying suspicious messages or links.
- Two-Factor Autentification: Add extra layers of security to accounts.
- Advanced Email Filtering: Use solutions that detect and block phishing attemps.
- URL Verification: Encourage users to verify links before clicking ensuring they come from legitimate domains.
- Incident Response Policies: Establish procedures to mitigate potential damage if a user falls victim to phishing