

# Types

## PHISHING vs SPEAR PHISHING vs WHALING

A COMPLETE GUIDE TO SOCIAL ENGINEERING ATTACKS

©Cyber Threat Intelligence

| PHISHING  | VS | SPEAR PHISHING   | VS | WHALING   |
|---|----|--|----|---|
| <p><b>1 FOCUS</b><br/><b>Broad &amp; Generic Attacks</b><br/>Aimed at mass audiences with general hooks; no research on individuals.</p>                         |    | <p><b>1 FOCUS</b><br/><b>Targeted &amp; Specific Attacks</b><br/>Aimed at specific groups or individuals; research-based and customized.</p>    |    | <p><b>1 FOCUS</b><br/><b>High-Level &amp; Extremely Targeted</b><br/>Aimed at C-suite executives, board members; deep research on profiles.</p>    |
| <p><b>2 DELIVERY</b><br/><b>Mass Distribution</b><br/>E.g., email blasts, SMS (smishing), automated voice calls (vishing); often automated.</p>                  |    | <p><b>2 DELIVERY</b><br/><b>Strategic &amp; Research-based</b><br/>Focused emails, social media messages to employees within a company or industry.</p> <p style="text-align: right;"><b>Strategic HARPOON</b></p>  |    | <p><b>2 DELIVERY</b><br/><b>Impeccably Strategic</b><br/>Extremely high-quality, legitimate-looking emails or BEC (Business Email Compromise).</p>   |
| <p><b>3 TACTICS</b><br/><b>Deceptive &amp; Urgency</b><br/>Impersonating banks, retailers, gov. agencies; creating fear to force actions (clicks, logins).</p>  |    | <p><b>3 TACTICS</b><br/><b>Personalized &amp; Convincing</b><br/>Uses known names, projects, interests; appears from trusted or external sources.</p> <p style="text-align: right;"><b>Customized logic</b></p>   |    | <p><b>3 TACTICS</b><br/><b>Authoritative &amp; Financial</b><br/>Requests large wire transfers, confidential financial reports, proprietary data; uses authority.</p>   |
| <p><b>4 TARGET</b><br/><b>Unsuspecting Individuals</b><br/>Customers, users, general employees; goal: large numbers of low-effort captures.</p>                |    | <p><b>4 TARGET</b><br/><b>Organizations &amp; Employees</b><br/>Mid-level staff, managers, HR, departments; goal: specific access or sensitive data.</p>    |    | <p><b>4 TARGET</b><br/><b>C-Level Executives</b><br/>CEOs, CFOs, COOs, Board Members; goal: massive financial gain or strategic information.</p>   |
| <p><b>5 FEATURES</b><br/><b>Low Cost, High Volume</b><br/>Relies on widespread distribution and human curiosity; easy to replicate.</p>                        |    | <p><b>5 FEATURES</b><br/><b>Higher Sophistication</b><br/>Requires reconnaissance and planning; more difficult to detect than generic phishing.</p>   |    | <p><b>5 FEATURES</b><br/><b>Ultimate Sophistication</b><br/>Requires months of planning; standard security filters often fail to detect; highest risk.</p> <p style="text-align: right;"><b>HARPOON</b></p>  |

**MODERN SECURITY APPROACH: Adopt Phishing Resistance & Threat Intel for Unified Protection**

Convergence unifies broad mass detection & deep targeted research for comprehensive social engineering visibility.

From:  
<https://wiki.fortier-family.com/> - Warnaud's Wiki

Permanent link:  
<https://wiki.fortier-family.com/cybersecurity/phishing>

Last update: 2026/04/26 17:59

