Common Threats & Attacks

COMMON THREATS & ATTACKS IN CYBERSECURITY



1. Social Engineering

- **Phishing** - Deceptive emails to steal credentials
- **Spooting** - Imitating trusted sources
- **Vishing** - Voice phishing over calls
- **Qujishing** - Malicious QR code redirection



2. Malware

- **Worms. Spyware, Adware** Data theft & survelliance
- **Ransomware** - Encrypting files for ransom
- **Trojans** - Malware disguised as legit software
- **Fileless Malware-** Operating in memory, hard to detect



3. Insider Threats

Employees or partners misusing access



Identity & Account Compromise

Credential Theft
Stolen passwords or session tokens



Advanced Threats

APT (Adyanced Persistent Threats) -Targeted prolonged attacks



Data Breaches

Unauthorized data exposure



Zero-Day Exploits

Unknown vulnerabilities



4. Advanced Threats

APT (Advanced Persistent Threats)
Targeted, prolonged attacks

DoS/DDoS Attacks
Flooding servers with traffic

Data Breaches
Unauthorized data exposure

Zero-Day Exploits
Attacks via third-party services

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

Permanent link:
https://wiki.fortier-family.com/cybersecurity/types

Last update: **2026/09/20 13:30**