**DUMPSTER DIVING**

1. An attacker cases an establishment and searches through trash bins, dumpsters, or areas where company information may have been accidentally discarded for information items which may be useful to the dumpster diver. The devastating nature of the items and/or information found can be anything from medical records, resumes, personal photos and emails, bank statements, account details or information about software, tech support logs and so much more. By collecting this information an attacker may be able to learn important facts about the person or organization that play a role in helping the attacker in their attack [1].
2. Organizations that do not take appropriate care with the destruction of hard copy information run the risk of confidential information falling into unauthorized hands. Instead of having such information destroyed securely, businesses may simply throw their confidential information (perhaps unwittingly) into the rubbish. An attacker may decide to raid the company’s dumpster and discover this information [2].
3. “Dumpster Diving,” the practice of rooting through a company or individual’s trash, can provide foreign and economic spies with valuable information that should have been discarded more carefully [3].

**REFERENCES**

1. <http://capec.mitre.org/data/definitions/406.html>
2. <https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931>
3. <https://archives.fbi.gov/archives/news/stories/2006/february/counterintel_021306>