

## 2.0 Binary Sleuths and Social Architects: Exploring OSINT and SE

### Glossary of Terms

Term	Definition
Advanced Persistent Threat (APT)	A prolonged and targeted cyberattack where an intruder gains unauthorized access to a network and remains undetected for an extended period to steal sensitive information.
Analysis	The detailed examination of processed data to extract meaningful insights. (OSINT step)
Baiting	A tactic that entices victims with a seemingly attractive offer or item to trick them into revealing sensitive information or downloading malware.
Collection	Using reconnaissance to gather information on a target from publicly available sources, such as social media. (OSINT step)
Dissemination	The reporting and distribution of analyzed intelligence to the intended recipients. (OSINT step)
Open-Source Intelligence (OSINT)	The process of collecting and analyzing information that's publicly available to gather insights.
Phishing	A form of cyber/social engineering attack where deceptive messages mimic legitimate sources to trick individuals into revealing sensitive information.
Preparation	Involves defining objectives, scope, and tactics for an OSINT effort. (OSINT step)
Pretexting	It involves creating a fabricated scenario to trick individuals into divulging information or performing actions they usually wouldn't.
Processing	Organizing and converting the collected data into usable formats. (OSINT step)
Quid pro quo	Leverages the psychological principle of reciprocity, where individuals feel obliged to return a favor or act in kind when something is provided to them.
Smishing	An attempt to deceive victim(s) through text messages, leveraging the widespread use and urgency associated with SMS messaging.
Social Engineering (SE):	Is the practice of manipulating individuals through psychological tactics to trick them into divulging confidential information or performing actions that compromise security.
Social Media Scraping	The process of extracting data from social media platforms, such as posts, user profiles, comments, and interactions, often using automated tools or scripts, to gather insights or conduct analysis.
Spear Phishing	A targeted form of phishing where attackers tailor their messages to specific individuals or organizations.
Tailgating	Involves an unauthorized person following an authorized individual into a restricted area, bypassing physical security measures.
Vishing	It uses deceptive phone calls to trick individuals into revealing sensitive information or performing actions that compromise security.

Whaling Attack	A type of spear phishing attack that targets high-profile individuals such as executives, government officials, or other important figures within an organization.
© 2024 Eric J. Magidson. All rights reserved.	

This Oregon SCC Grant Consortium product is funded by a \$5 million Strengthening Community Colleges Employment and Training Administration Grant from the U.S. Department of Labor. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The U.S. Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability, or ownership. This product is copyrighted by the institution that created it.