Phishing Analysis Glossary

This document is designed to cover acronyms and terms used in the Phishing Analysis domain of the Blue Team Level 1 certification training course.

This document is TLP:White, and can be shared without breaching the Terms and Conditions of the BTL1 course.

Learn more about Blue Team Level 1 and purchase the certification here – https://securityblue.team/why-btl1/

IOC // **Indicator of Compromise** – Intelligence gathered from malicious activity, intrusions, or incidents. An example would be a piece of malware that was observed in an attack against an organization. The file hashes and file name can be shared with other organizations so they can add it to blocklists or perform threat exposure checks.

Artifact // An important piece of information retrieved from data, such as an email, website, or file. This includes value such as; email addresses, sending server IPs, file hashes, and domain names.

File Hash // The unique text string that is generated by a hashing algorithm is used on a file, such as MD5, SHA1, or SHA256. The current standard in industry is SHA256 as it does not suffer from hash collisions.

Recon // **Reconnaissance Phishing Email** – An email that is trying to get the user to respond, or simply being sent to see if the recipient mailboxes are registered and in use. A good way to identify potential targets for future phishing attacks.

Cred Harvester // **Credential Harvester Phishing Email –** An email that convinces recipients to click on a hyperlink and visit a website where they need to enter in their account details, where the website typically masquerades as known brands such as Amazon, PayPal, and government services.

Vishing // **Voice Phishing –** Instead of using email, these attacks use voice calls and social engineering techniques to convince targets to complete an action they would likely not normally conduct, such as providing information or visiting a malicious website.

Smishing // **SMS Phishing –** Instead of using email, these attacks use text messages and social engineering techniques to convince targets to complete an action they would likely not normally conduct, such as providing information or visiting a malicious website.

BEC // **Business Email Compromise –** This term means different things to different people. The primary uses are to explain a scenario where an email mailbox owned by an organization is hacked and used to send phishing emails or retrieve information from the mailbox, or is used to describe any phishing attack against an organization.

SPF // **Sender Policy Framework -** A Sender Policy Framework (SPF) record is a type of DNS (TXT) record that can help prevent an email address from being forged by alerting recipients that the email is not from the domain it appears to be from.

DMARC // **Domain-based Message Authentication, Reporting and Conformance -** DMARC is an email authentication, policy and reporting protocol. This protocol can specify what happens when an email fails SPF and DKIM checks (quarantine, reject, allow).

DKIM // **DomainKeys Identified Mail –**DKIM is a method of email authentication that cryptographically verifies if an email has been sent by its trusted servers and hasn't be tampered during transmission.