Kroll

Most Frequently Used Cyber Terms

A baseline glossary of words and phrases used in relation to cyber attack or data compromise.

CYBER TERM	DEFINITION*
BLACKLIST	A list of email senders who have previously sent spam to a user. SOURCE: SP 800-114
	A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity. SOURCE: SP 800-94
BRUTE FORCE PASSWORD ATTACK	A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords. SOURCE: SP 800-72
DISTRIBUTED DENIAL OF SERVICE — (DDOS)	A Denial of Service technique that uses numerous hosts to perform the attack. SOURCE: CNSSI-4009
END-TO-END ENCRYPTION	Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible. SOURCE: SP 800-12
	Encryption of information at its origin and decryption at its intended destination without intermediate decryption. SOURCE: CNSSI-4009
MALWARE	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. SOURCE: SP 800-83
	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. SOURCE: SP 800-61
MULTIFACTOR AUTHENTICATION	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). SOURCE: SP 800-53
PHISHING	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. SOURCE: SP 800-83
	Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. SOURCE: CNSSI-4009
	A digital form of social engineering that uses authentic-looking — but bogus— emails to request information from users or direct them to a fake Web site that requests information. SOURCE: SP 800-115

Most Frequently Used Cyber Terms, continued.

CYBER TERM	DEFINITION*
SKIMMING	The unauthorized use of a reader to read tags without the authorization or knowledge of the tag's owner or the individual in possession of the tag. SOURCE: SP 800-98
SOCIAL ENGINEERING	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. SOURCE: SP 800-61
	A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. SOURCE: SP 800-114
	The process of attempting to trick someone into revealing information (e.g., a password). SOURCE: SP 800-115
	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack an enterprise. SOURCE: CNSSI-4009
WHITELIST	A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system. SOURCE: SP 800-128

* REFERENCE
Kroll has assembled these most frequently used items from the NIST Glossary of Key Information Security Terms, extracted from NIST Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, and from the Committee for National Security Systems Instruction 4009 (CNSSI-4009), among others. Updated versions of the NIST Glossary will be posted on the Computer Security Resource Center (CSRC) Web site at http://csrc.nist.gov/.

These materials have been prepared for general information purposes only and do not constitute legal or other professional advice.
Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have.

CONTACT

Jennifer Rothstein, Director, Insurance Channel Management, Cyber Security and Breach Notification
jrothstein@kroll.com | T +1 212.833.3456

kroll.com