Quick Guide

IT Security Terms and Definitions

Part of what can often make technology seem confusing is the terminology that goes along with it. As with sports medicine or any other specialized area, technology comes with its own shorthand, both basic and complex. A working knowledge of basic IT security terms can go a long way towards not only helping you communicate better with your IT provider, but helping you to understand what your business' security risks are and how to protect yourself and your business from them.

Here are a few of those basic terms:

Access Control – Access Control allows you to set restrictions that will keep important information and applications from being accessed by unauthorized users.

Authentication – Authentication refers to any process that confirms the identity of a user or the authenticity of login credentials and passwords.

Biometrics – Biometrics are physical characteristics used in the authentication process, such as fingerprints or facial recognition.

Botnet – A botnet is a large number of compromised computers that are used by cybercriminals to create and send spam or viruses, or flood a network with messages as part of a Denial of Service attack.

Brute Force – A style of cyber-attack that consists of any kind of attack method that involves trying any and all available possibilities one-by-one until a system or network is breached successfully.

Business Continuity Plan – A plan for emergency response, backup operations, and post-disaster recovery steps that will keep critical resources available and facilitate the continuity of operations in an emergency situation.

Decryption – Decryption is the process of translating an encrypted message back into its original plaintext.

Denial of Service – Often called a DoS Attack, Denial of Service is when access to a system resource is blocked, or system operations and functions are slowed down significantly due to a sudden and massive overload of the system in question. This tactic is commonly used to shut down websites.

Disaster Recovery Plan – A Disaster Recovery Plan is a process put in place to recover and restore IT systems in the event of a disruption or disaster.

Encryption – The cryptographic transformation of data – or plaintext – into ciphertext, which makes data unreadable to anyone who accesses that data without authorization.

Firewall – A logical or physical roadblock in a network that prevents unauthorized access to data or resources.

(888) 727-1994, ext. 3 • info@L5Consulting.com
www.L5Consulting.com

L5 CONSULTING
TECHNOLOGY & OPERATIONS MANAGEMENT

Hyperlink – Typically a line of text, but sometimes an image, a hyperlink is a clickable shortcut to a specific web address. Text hyperlinks are typically shortened to be easier to read or changes into unrelated text, but hovering your mouse over the hyperlink will reveal the complete "original" address.

Malicious Code – Software that presents a something innocuous, but actually grants a hacker unauthorized access to system resources or tricks a user into executing other malicious functions on the hacker's behalf.

Malware – A generic term for a wide range of different types of malicious code.

Penetration Testing – A method of testing the external perimeter security of a network or facility to see how well security measures can keep intrusions out.

Phishing – The use of emails that seem to be sent from a trusted source to trick a user into doing something like entering valid credentials at a fake website, sharing confidential information, or granting access to funds or other company resources.

Risk Assessment – A process that identifies potential security risks and the impact of those risks could have on a business.

Social Engineering – Refers to any type of non-technical or low-technology means used to carry out a cyber-attack such as lies, impersonation, tricks, bribes, blackmail, and threats.

Spam – Electronic junk mail that can often contain malicious content.

Spoofing – A tactic used to gain access to a system by posing as an authorized user, and a frequent component of Phishing and Social Engineering attacks.

Trojan Horse – A computer program that seems legitimate on the surface, but contains a hidden and potentially malicious function that evades security measures, often by exploiting legitimate program or system functions.

User – A generic term for a person, entity, or automated process that accesses a system, whether authorized to do so or not.

Virus – A hidden, self-replicating section of computer software that spreads by infecting another program. A virus requires that its "host" program be run to make the virus active.

Worm – A computer program that can run independently and embed a complete working version of itself onto other hosts on a network. Worms often consume and destroy data and resources in their path.

Zero Day – An exploit for which no patch is available yet. Zero Day exploits are new or unknown vulnerabilities in a program that can be used to gain access to systems, networks, and devices.

We are the IT security experts that businesses trust. To learn more about what you can do to protect your business against cyber threats, contact L5 Consulting at info@L5Consulting.com or (888) 727-1994, ext. 3