# Cyber Glossary

Cyber/Internet/Networking Terms

Willis

# Contents




For further information, contact:

Geoffrey Allen

Senior Vice President/e-Solutions Practice Leader

Telephone: 212 837 0745

Email: allen_gk@willis.com

# Cyber Glossary

Browser: A software application used to view and interact with the web.

Cookie: Code which is transferred to an internet user's computer when visiting a web site.

Cyber Liability: Third-party coverage for liability arising from the failure of an insured to prevent unauthorized use or access of it its network; transmission of a computer virus to a third party; theft of confidential information; or denial-of-service.

Cybersquatting: Use of trademarks belonging to others in registering a domain name (a web site's address on the web).

Denial of Service: Action preventing an information system from functioning in accordance with its intended purpose, i.e. flooding a system to prevent it from servicing normal and legitimate requests.

Extranet: Limited access to a company's intranet given to other companies or the public.

Framing: Using hyperlinks to use another party's web site content to display one's own advertising.

Hacker: A person compromising computer security or gaining unauthorized access to a computer file or system.

HTTP: Hyperlink transfer protocol, which allows words, graphics, video and sound to be transmitted via the web.

Hyjacking: Where an active, established session is intercepted and co-opted by an unauthorized user.

Internet: A three-level hierarchy composed of backbone networks, mid-level networks and stub networks, which includes many different physical networks worldwide.

Intranet: An internal TCP-IP network used for sharing information within an organization; not necessarily connected to the internet.

ISPs: Internet service providers – companies providing access to the internet.

Linking: Process by which a web site user clicks on a "link" (an icon, or underlined/highlighted text) and is transferred to another web page.

Logic Bomb: A computer program which is resident on a system and when executed, checks for a particular condition or particular state of the system which, if satisfied, triggers the perpetration of an unauthorized act.

Malicious Code: Hardware, software, or firmware that is intentionally inserted into a system for an unauthorized purpose; e.g. a Trojan horse.

Metatags: Hidden code embedded into web pages that enable search engines to quickly gather information about the pages.

Network: The hardware and/or software making up a data communications system.

Portal: Web site providing an entrance to the web usually by offering a search engine or useful links.

Public Key: Method of encryption that uses a closed combination key that encrypts messages and an open combination key that decrypts the messages.

TCP/IP: The data transmission standard used on the internet, which uses transmission control protocol and internet protocol.

URL: Uniform resource locator – the full internet address of an internet file.

Virtual Private Networks (VPN): Networks that are essentially private, but use the internet in lieu of expensive leased phone lines between offices.

Virus: A program that can infect other programs by modifying them.

Worm: A program that replicates from machine to machine across network connections, often-clogging networks and information systems as it spreads.