GLOSSARY

IT Security Foundations: Core Concepts

With Lisa Bock

Use the terms and definitions below to understand concepts taught in this course.

Transcript Search: note that you can search for terms spoken by the instructor during the course. To search videos, switch to the Transcript tab, then search for keywords using the In this video or In this course option.

Term	Definition
Risk	A function of a threat exploiting a vulnerability according to a formula: Risk = Threat X Vulnerability
Threat	Anything that can exploit a vulnerability, either Intentionally or accidentally, and can range from innocent mistakes made by employees to natural disasters, which in general are difficult to control
Vulnerability	A security flaw or weakness in a system that can be exploited by threats in order to gain unauthorized access to an asset, and can include unpatched systems, human error, or software flaws
Virus	A malicious program that can alter the integrity of a system. The results can be as simple as a new icon on the desktop or more serious results such as disabling antivirus or destroying files
Worm	Self-replicating malware that can spread through the network without any help from a transport agent
Spyware	Tracks information on a user's viewing habits while on the internet, and then sends that information to a remote computer without the user's knowledge
Trojan	A program that appears to be innocent but has been designed to cause some malicious activity, or provide a backdoor to your system

Zero-day vulnerability	Occurs when a malicious actor takes advantage of a software vulnerability that is unknown or undisclosed by the software vendor
Rootkit	A collection of programs that can infiltrate a computer system, create a backdoor and remain undetected, which can allow a hacker to take administrator level control of the victim's computer
Cookies	Small text files used by most major websites to store state information to preserve information about preferences and sign-in information
Confidentiality	The promise of keeping private information private by preventing unauthorized access
WI-FI protected access (WPA)	An encryption method used to secure wireless transmissions. As of 2018, WPA3 provides the most robust protection and is the preferred standard
Asymmetric Encryption	Asymmetric Encryption is one of the two main types of encryption. It is also called Public Key encryption uses two keys, a public key and a private key, which are mathematically related
Symmetric Encryption	Symmetric encryption is one of the two main types of encryption. It is also called conventional encryption and uses a single, shared, secret key
Integrity	Protecting data from unauthorized modification