NOVA CYBERSECURITY LAB GLOSSARY

The Cybersecurity Lab contains terms that may be unfamiliar to educators and students. In the game, these terms are highlighted with definitions that appear as mouse-overs. Below is a list of these terms and their definitions:

Antivirus software
Computer programs that can block, detect, and remove viruses and other malware.

Backups/backing up files
Extra copies of computer files that can be used to restore files that are lost or damaged.

Bandwidth
The amount of data that can pass through a network or part of a network per second.

Botnet
Multiple computers on a network that are infected with a program that can be controlled remotely. The infected computers are usually used to cause damage that couldn't be achieved with a single computer.

Computer network
Two or more interconnected devices that can exchange data.

Computer virus
A computer program that can copy itself and cause harm in various ways, such as stealing private information or destroying data.

DDoS
A distributed denial of service attack attempts to make an online service, like a website, unavailable by overwhelming it with a flood of traffic from a team of computers.

Doxnet
A fictional virus modeled after the Stuxnet virus. Like Stuxnet, Doxnet is able to damage physical infrastructure.

Encryption
The process of using codes to make readable information unreadable. Encrypted information cannot be read until it is decrypted using a secret key.

Firewall
Software designed to block malware from entering protected networks.

Hacktivist
Someone who uses computers and computer networks to disrupt services or share secret information in an effort to draw attention to political or social issues.

Internet service provider (ISP)
A company or organization that gives users and devices access to the Internet.

Support for the Cybersecurity Lab is provided by Lockheed Martin. NOVA is produced for PBS by WGBH in Boston.

LOCKHEED MARTIN WGBH

NOVA CYBERSECURITY LAB GLOSSARY

The Cybersecurity Lab contains terms that may be unfamiliar to educators and students. In the game, these terms are highlighted with definitions that appear as mouse-overs. Below is a list of these terms and their definitions:

Keylogger malware
A program that records every key struck on a keyboard and sends that information to an attacker.

Malware
Software that harms computers, networks, or people. Includes viruses, worms, ransomware, and other computer programs.

Phishing
Attempting to trick people into revealing sensitive information, such as passwords and credit card numbers, often by using emails or fake websites that look like they are from trusted organizations.

Ransomware
A type of malware that holds victims' computer files hostage by locking access to them or encrypting them. It then demands a ransom if the victim wants his or her files back.

Server
A computer or computer program that provides specific services on a network, such as an email server that directs emails and a web server that serves up web pages.

Software
Consists of code written in a programming language that instructs computers to perform specific tasks.

Software patch
A piece of software designed to update a computer program in order to fix a software vulnerability or improve the program.

Software vulnerability
A flaw or weakness in a computer program that hackers or malware can exploit to gain access to a system or damage it.

Spam
Unsolicited emails sent to many addresses. The purpose of most spam is to make money through advertising or identity theft.

USB drive
A data storage device that is used to store, back up, and transfer computer files.

USB port
A type of connection between devices that can exchange information and power supply.

Support for the Cybersecurity Lab is provided by Lockheed Martin. NOVA is produced for PBS by WGBH in Boston.

LOCKHEED MARTIN WGBH