Trojan:
Assume you receive an email from your bank with an attachment that appears to be an invoice. When you open the attachment, malware is installed on your computer that steals your personal information.

Traceroute:
Assume you are having difficulty connecting to a website. Traceroute is used to determine the path that your data takes to reach the website. You discover that there is a problem with one of the routers on the path.

Tunnel:
For example, suppose you are using a public Wi-Fi network and want to ensure that your traffic is encrypted. You use a VPN tunnel to encrypt your traffic and protect your privacy.

Virtual Private Network (VPN):
Assume you are traveling for work and need to connect to your company's network. You use a VPN to securely connect to your company's network from anywhere in the world.

Virus:
Suppose you open an email attachment containing a virus. The virus replicates and spreads to other computers on your network.

Vulnerability:
Example: An attacker can obtain your personal information by exploiting a vulnerability in your web browser. To address the vulnerability, you must update to the most recent version of your web browser.

War Driving:
Using a laptop and a wireless network adapter, an example hacker searches for unprotected wireless networks as they drive through a city. After that, they join the networks and take advantage of the computers connected to them to steal data.

WHOIS:
Say you would like to know who owns a website. You can find the website owner's contact details by using WHOIS.

Wireshark:
For instance: You are diagnosing and resolving a network issue. In order to locate the problem's origin, you can use Wireshark to record and examine network activity.

Worm:
Example: A worm uses the vulnerabilities in other computers to replicate itself and spread to other systems. Worms can cause widespread damage to computer systems.

The Wireless Application Protocol (WAP):
For instance, let us say you are accessing the internet via a smartphone. Delivering web content to mobile devices is done via the WAP protocol.

Web Application Firewall (WAF):
An illustration of a security tool used to defend web applications against attacks is a WAF.

Zero-Day:
As an instance, a zero-day vulnerability is one that the software vendor is unaware of. This means that there is no patch available to fix the vulnerability.

Zombie:
A zombie, for example, is a computer that has been infected with malware and is controlled by an attacker. Zombies can be used to launch denial-of-service attacks or other attacks.