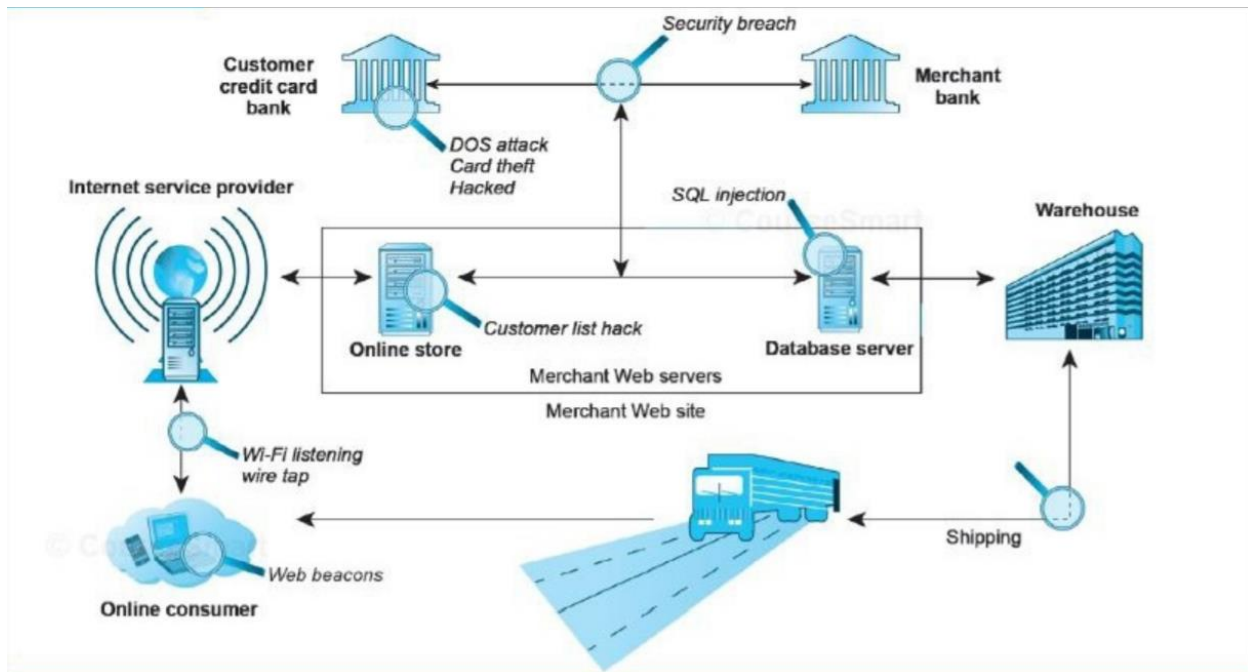


## SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline.



There are three major vulnerable points in e-commerce transactions: Internet communications, servers, and clients.

## MALICIOUS CODE

**Malicious code** (sometimes referred to as "malware") includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots.

**Drive-by download** - A drive-by download is malware that comes with a downloaded File that a user intentionally or unintentionally requests. Drive-by is now one of the most common methods of infecting computers.

**Virus** - A virus is a computer program that has the ability to replicate or make copies of itself, and spread to other files. In addition to the ability to replicate, most computer viruses deliver a "payload." The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive—destroying files, reformatting the computer's hard drive, or causing programs to run improperly.

**Worm** - Viruses are often combined with a worm. Instead of just spreading from file to file, a worm is designed to spread from computer to computer. A worm does not necessarily need to be activated by a user or program in order for it to replicate itself.

**Ransomware** - Ransomware (scareware) is a type of malware (often a worm) that locks your computer or files to stop you from accessing them. Ransomware will often display a notice that says an authority such as the FBI, Department of Justice, or IRS has detected illegal activity on your computer and demands that you pay a fine in order to unlock the computer and avoid prosecution.

**Trojan horse** - A Trojan horse appears to be benign, but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate, but is often a way for viruses or other malicious code such as bots or roorkits (a program whose aim is to subvert control of the computer's operating system) to be introduced into a computer system.

**Backdoor** - A backdoor is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer. Downadup is an example of a worm with a backdoor, while Virut, a virus that infects various file types, also includes a backdoor that can be used to download and install additional threats.

**Bots** - Bots (short for robots) are a type of malicious code that can be covertly installed on your computer when attached to the Internet. Around 90% of the world's spam, and 80% of the world's malware, is delivered by botnets. Once installed, the bot responds to external commands sent by the attacker;

**Botnets** -Botnets are collections of captured computers used for malicious activities such as sending spam, participating in a DDoS attack, stealing information from computers, and storing network traffic for later analysis. The number of botnets operating worldwide is not known but is estimated to be well into the thousands.

## **POTENTIALLY UNWANTED PROGRAMS (PUPS)**

In addition to malicious code, the e-commerce security environment is further challenged by **potentially unwanted programs (PUPs)** such as adware, browser parasites, spyware, and other applications that install themselves on a computer, such as rogue security software, typically without the user's informed consent. Such programs are increasingly found on social network and user-generated content sites where users are fooled into downloading them.

**Adware** is typically used to call for pop-up ads to display when the user visits certain sites. While annoying, adware is not typically used for criminal activities. ZangoSearch and PurityScan are examples of adware programs that open a partner site's Web pages or display the partner's pop-up ads when certain keywords are used in Internet searches.

A **browser parasite** is a program that can monitor and change the settings of a user's browser, for instance, changing the browser's home page, or sending information about the sites visited to a remote computer. Browser parasites are often a component of adware. For example, Websearch is an adware component that modifies Internet Explorer's default home page and search settings.

**Spyware**, on the other hand, can be used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screen shots (and thereby capture passwords or other confidential data).

## **PHISHING**

Social engineering relies on human curiosity, greed, and gullibility in order to trick people into taking an action that will result in the downloading of malware.

Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain. Phishing attacks typically do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so-called "social engineering" techniques. One of the most popular phishing attacks is the e-mail scam letter. The scam begins with an e-mail: a rich former oil minister of Nigeria is seeking a bank account to stash millions of dollars for a short period of time, and requests your bank account number where the money can be deposited. In return, you will receive a million dollars.