**Windows Firewall:**

A firewall, at its most basic level, permits or denies communications between computers, between networks, or between computers and networks (for example, your home computer and the Internet) based on the firewall’s configuration rules. You can access the settings for Windows Firewall through the Network and Security section in the Control Panel.

Almost all computers and networks communicate by establishing connections between two hosts using an IP address and a port. Although there are many types of firewalls, the most common type of firewall (and the type used in Windows 7, provided by Windows Firewall) permits or denies communications based on IP address and port information.

Only connections that are explicitly allowed, using firewall rules, are permitted. Windows Firewall, by default, allows all *outbound* connections, and permits only *established inbound* connections (that is, an inbound connection that is in direct response to an outbound connection initiated from your computer or network).

There are firewalls protecting Microsoft’s Web servers and your ISP’s DNS servers. In order for your computer to connect to Microsoft’s Web servers, Microsoft must first create firewall rules to allow the communication. This is accomplished by creating a firewall rule that essentially says to allow any inbound IP address to connect to 207.46.232.182 (Microsoft’s Web server) on port 80 (HTTP). Your ISP must create a similar rule on their firewall that essentially says to allow any inbound IP address to connect to its DNS servers on port 53 — which is the standard port for DNS.

Windows Firewall permits your outbound DNS request to your ISP’s DNS server, and your computer’s outbound HTTP request to Microsoft’s Web server. In your outbound request, your computer first sends the DNS request to your ISP’s DNS server on port 53, and tells your ISP’s DNS server on what port it will be listening for a response.

Your computer selects a random port number between 49,152 and 65,535, and Windows Firewall automatically creates a temporary rule that allows an inbound connection from the IP address of your ISP’s DNS server to the IP address of your computer, on that random port number.

After the response is received (or if a response is not received within a specified period of time, say 30 seconds), the rule is automatically deleted from the firewall and the connection is again blocked. A similar process is then repeated to connect to Microsoft’s Web server