How do computers connect to each other over the Internet?

In the last issue, I described how a request for a webpage is sent from your computer to the host site of the webpage. But how does that webpage know to send it back to your computer? This is where an IP address is used.

IP address (Internet Protocol)

An IP address identifies each networked computer and device on a network. When you sign up with an Internet service and connect your modem, your internet provider assigns you a public IP address. This address is how you communicate with all the other devices out there on the public Internet. But, you've likely got multiple computers and other devices on your network—each of which has its own private IP address.

The first step is your public IP address. When you log onto your internet connection your internet provider gives you a public IP address. This is used to identify your computer on the Internet. It works like a return address would on a piece of mail. You send a request out to a website. When your computer or device sends a request, it tags the request with your public IP address. That way the website knows where to send the response. This public IP address is not permanent. Should you log off and log on again later this public IP address will most likely be a different IP address.

This is also how your internet provider knows who you are and can see what you are doing and use that information for monitoring your internet usage and for billing.

The second step is your private IP address. Your computer also has a separate IP address, your private IP address. If you have more than one computer on a wifi network then each will have a specific private IP address. This is supplied by your router. When the request returns it goes to your router which then directs it to the correct computer based on the private IP address of that computer.

If you want to hide your public IP address (from your provider, hackers etc) there are a number of ways to do this:

1. Use a VPN (virtual private network) – the best and most secure method
2. Use the TOR browser – the slowest but also secure
3. Using a proxy server – a riskier method
4. Using a public/free wifi – a potentially dangerous method

More on using these methods in a later newsletter.

Cookies

Cookies are small text files, ID tags, that are stored on your computer's browser. Cookies are created when you use your browser to visit a website that uses cookies to keep track of your movements within the site, help you resume where you left off, remember your registered login, theme selection, preferences, and other customization functions. The website stores a corresponding file (with same ID tag) to the one they set in your browser, so they can track and keep information on your movements within the site and any information you may have voluntarily given while visiting the website, such as any registration information and/or your email address.
Most commercial sites probably use cookies. Some will give a message on their page that cookies are used on this site. Some sites demand you accept their cookies prior to accessing their site.
There are two types of cookies, either primary of third party. Every browser has, in its settings, the ability to block cookies (along with history etc) but I recommend only having the setting activated to block third party cookies.
Primary cookies are the ones downloaded from the site your visiting. These can be useful to if you regularly visit that site as your details are known and your browsing will be faster. The disadvantage is that they can target you with ads based on your previous browsing experience. But if it's a site that requires some type of registration such as a password then that will be remembered by the site and you won't need to re-enter every time. Any registration details such as a password will eventually expire for that site and you'll need re-register but it shouldn't be for some time. I have sites that re-request a password on a yearly basis.
Third party cookies are for sites on the webpage operated by other parties. Often found as advertisements or videos. Clicking into one of these may result in them downloading a cookie onto your browser. Unless you want their cookie, they may be just annoying. I have my browsers set to block third party cookies.
Cookies can be deleted from the browser settings page or by using cleaning programmes such as Ccleaner. Another option is to use the browsers private browsing facility. Every browser has this ability. Using this method any information the website has from your session is lost when you exit the browser.

Peter Day