Important Web Basics Affecting Your Computer Security by Peter McKiel

Article published on November 30th 2011 | Software

With our increasing dependence on computing devices and the Internet to run our lives, itâ€™s essential to have the right know-how to keep your personal information protected against malware theft.

Part 1 of this guide series looked at the workings of Hosts, IP addresses, DNS, ISPâ€™s and the Backbone.

The following guide will continue to explore some key Web terms to better enable you to keep your computer or network safe. We will cover protocols and related activities which enable computers to talk to each other, as this will help you understand how they can be used against you by cyber criminals.

Protocols - TCP/IP

Protocols are the term given to the set of conventions governing the treatment and formatting of data in electronic communications systems. Basically, this boils down to the fact that without protocols, computers cannot communicate with each other online.

To clarify further with an analogy - if you call an orange a banana and I call it a pear, we would never be able to understand each other - a common agreement has to be made as to what we will both call it.

Translated to computers and the Internet, different organisations have their own proprietary way of formatting and transmitting data, so there has to be a protocol for all computers to speak the same language.

Transmission Control Protocol Internet Protocol (TCP/IP) is the accepted set of communication standards that act as a â€˜universal translatorâ€™ if you will. It comes packaged by default with all major computer operating systems.

As we have previously discussed in the last guide, IP relates to the unique address of your computer which identifies it on the Internet so that communications can reach you. TCP is responsible for breaking data into smaller chunks called packets for easier transfer between different computing devices. It then reassembles these multiple packets in the correct sequence and performs error-checking to ensure that the complete data message arrives intact at its destination.

DHCP

In the early days of the Internet, IP addresses were manually coded to each computer. But once the web exploded in popularity it became extremely tricky to track which IP addresses were already in use and which ones were freed up when a computer was removed from the network.

Dynamic Host Configuration Protocol (DHCP) was then created to automate this process. Thus, a DHCP server is given a block of IP addresses that it manages. In this way, your Host (which delivers web pages) will contact the DHCP server when you turn your computer on to request an IP address. The DHCP server will then check its database of IP addresses and find one that is not in use to assign to your Host.

NAT

As more and more people in the world are now using computers online, inevitably the issue arises of IP addresses running short. While a newer IP protocol is under development which will allow for exponential increases in available IP addresses, in the mean time something called Network Address Translation (NAT) is used to tackle this problem. NAT essentially reduces the IP addresses on a local network to a single IP for external use.

To clarify further, without NAT, a company with 1000 computers that wanted all of them to be connected with the Internet would need to have 1000 separate public IP addresses. But using NAT, the company will only need 1 public IP address recognised on the Web, while all the computers on its internal network will still be uniquely recognised by each other but their IP addresses will be hidden from external view.

This hiding of internal IP addresses not only allows for more Hosts to share the Internet, it also adds an extra layer of security. This is because by not allowing the outside world to know the exact IP addresses on your internal network, you take away a crucial piece of information that cyber criminals could use to hack your system.

Conclusion

In summary of the above guide, you will now know that protocols are what allow for standardised communication between computers, that TCP/IP is the collection of these protocols and that NAT gives added cyber protection by allowing computers on the same network to hide their unique IP addresses from the outside world. With all this complexity going on in the background to facilitate the electronic transfer of information, you can also now understand that antivirus software acts as a brave soldier guarding against unauthorised breaches while computing devices communicate with each other.

Article Source:
http://www.articleside.com/software-articles/important-web-basics-affecting-your-computer-security.htm - Article Side

Peter McKiel - About Author:
Peter McKiel is an independent IT Consultant. He research on a antivirus software

Article Keywords:
antivirus software