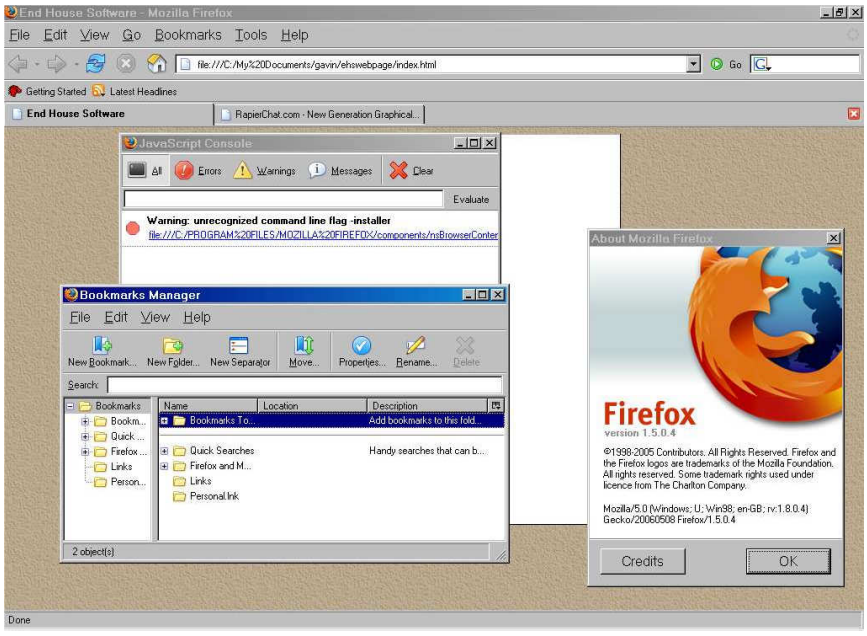
TECH EXCHANGE No. 2 – The Internet Made Simple (part 1)

This will be a two-part column in which I will to explain the technology behind the biggest international network - the Internet.

The Internet started in the late 1960s as a military experiment. The idea was to create a robust computer network that could withstand a nuclear attack. The network could survive the loss of machines without compromising the ability of the remaining machines to communicate. The result was a success but was limited in scope. Only defense contractors and academics could gain access to what was then known as the ARPAnet (Advanced Research Agency network of the Department of Defense). Two main events then happened to create the Internet we all know today. During the early 1990s some physicists at CERN, the European Particle Physics Laboratory, released a language developed to enable creating and sharing of multimedia (text, images and sound) documents. So was born the base language of the Internet – HTML (Hypertext Markup Language). Meanwhile some bright students at NCSA (National Center for Supercomputing Applications) wrote a web browser called Mosaic. With versions based on easy-to-use graphical interface which is familiar to today's computer users. Millions of users grab a copy of this free browser and began surfing the Internet. Also during this time we see the introduction of high-speed modems for digital communication over the phone lines.

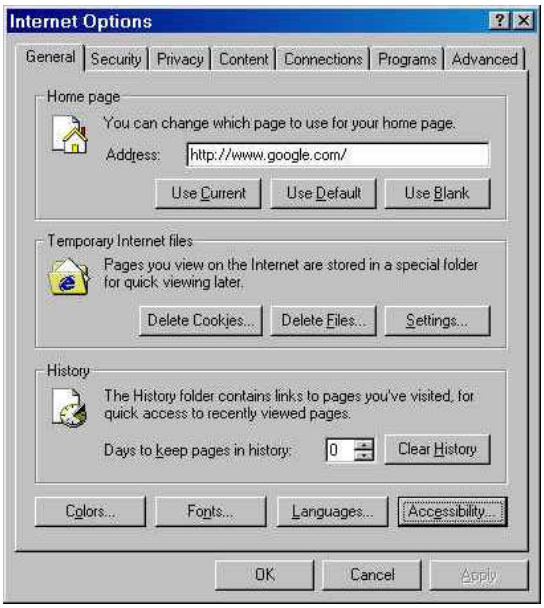
The Internet Engineering Task Force (IETF) is responsible for defining and managing Internet technologies. The technology is defined in documents known as Requests For Comments (RFC). RFCs are individually numbered and describe everything from the syntax of domain names to the format of electronic mail messages (email). To learn more about the IETF visit http://www.ietf.org. The World Wide Web Consortium (W3C) was formed with the charter to define that standards for HTML (see part 2) and other technology related to the world wide web. To learn more about the W3C visit http://www.w3.org.

The most common piece of Internet browser software is of course Microsoft's Internet Explorer (version 7 of which is now in beta testing). So why would you want to use another browser? The answer is that the new browsers coming to the marketplace are adding new features that IE are now only catching-up with. The most common new feature is 'tabbed' browsing. In the current version of IE, every website you view replaces the current one – the only way of keeping a webpage is to add it to the favorites or opening another copy of IE. With tabbed browser, every website you view becomes a tab displayed along the top of the screen but in the same copy of IE. To view a pervious website you just click on the appropriate tab.



A browser receiving coverage in the press now is Mozilla Firefox available at (http://www.mozilla.org), which now accounts for about 10% of the browser market. Firefox is based on the 'open-source' design philosophy – where the source code is freely available and can be modified and extended by anyone in the developer community. This produces free software that is unconstrained by the likes of large companies. In the case of Firefox, this has produced a wealth of add-ons covering areas from RSS (Rich Site Summary – see part 2) to Gmail (Google Mail). There are now over 1000 add-ons available at http://addons.mozilla.org/firefox. Firefox of course includes tabbed browsing as described above.

It goes without saying that you should use your common sense when browsing the Internet. I would like to bring one type of fraud to your attention - phishing. This type of fraud is becoming a common practice. It usually involves receiving a email (or viewing a webpage) purporting to be from an official source, e.g. your bank stating that they have had a computer crash and have lost your internet banking details. They supply a link that if followed would display a webpage containing a form requesting you to renter your details, e.g. your password. The webpage would look genuine, copying the style of your bank's webpages even down to using the bank's logo. BUT the webpage is NOT GENUINE – if you filled in the form, the information would be sent directly to the criminal and they would log on to your Internet banking account and clean it out! An official source WOULD NEVER request personal information in this manner. When you log on to for example your Internet banking service always type the full addresses (URL) as supplied by the bank into the browser and NEVER click on a link.



A website can store small pieces of information in what we call a 'cookie', that will exist stored on your hard disk between visits to that website. This can be as simple as recording your particular preferences for that website, like the colour scheme or font size for example. The privacy issue arises when cookies are used to store say your searching history and preferences. This information is used to display targeted adverts on some websites. This might be fine if you are the only one to use the computer, but if many people use the computer, you might not want people to know what you were searching for ...

To clear the audit trails from within Internet Explorer (IE), select 'Internet Options...' from the Tools menu. This displays a dialog box as shown in the screen shot. From here you can select to clear history, cookies and the temporary download folder. You will need to restart the browser and in some causes reboot the computer for the changes to take effect.

To protect your privacy, many products have sprung up, claiming to remove all the audit trails – recycle bin, cookies, browser history, etc. Two I have had experience with are Window Washer (see screen shot) from Web Root Software (http://www.webroot.com) and Evidence Eliminator (http://www.evidence-eliminator.com).

In part 2 we will cover common problems encountered while browsing and ways of enhancing your browsing experience. This week's recommended site is NTBUGTRAQ (http://www.ntbugtrag.com). This is a mailing list maintained by Russ Copper. It details all the latest bug reports and patches for the Windows operating system. When you sign up you receive regular emails detailing all the latest security news. The site also contains pointers to software tools that can be used to determine a system's vulnerability. That's it for this week, please send any questions or comments to techexechange@endhousesoftware.com.

By Gavin Baker.