Parental Controls:

Several techniques exist for creating parental controls for blocking websites. Add-on parental control software may monitor API to observe applications such as a web browser or Internet chat application and intervene according to certain criteria, such as a match in a database of banned words. Virtually all parental control software includes a password or other form of authentication to prevent unauthorized users from disabling it.

Techniques involving a proxy server are also used. A web browser is set to send requests for web content to the proxy server rather than directly to the webserver intended. The proxy server then fetches the web page from the server on the browser's behalf and passes the content to the browser. Proxy servers can inspect the data being sent and received and intervene depending on various criteria relating to the content of the page or the URL being requested, for example, using a database of banned words or banned URLs. The proxy method's major disadvantage is that it requires that the client application be configured to utilize the proxy. This control is easily bypassed if the user can reconfigure applications to access the Internet directly rather than through the proxy. Proxy servers themselves may be used to circumvent parental controls. There are other techniques used to bypass parental controls.

The computer usage management method, unlike content filters, is focused on empowering the parents to balance the computing environment for children by regulating gaming. The main idea of these applications is to allow parents to introduce a learning component into the computing time of children, who must earn gaming time while working through educational content.

Lately, network-based parental control devices have emerged. These devices work as a firewall router using packet filtering, DNS Response Policy Zone (RPZ) and Deep packet inspection (DPI) methods to block inappropriate web content. These methods have been used in commercial and governmental communication networks. Another form of these devices made for home networks has been developed. These devices plug into the home router and create a new wireless network specifically designed for kids to connect to.

Parental controls on mobile devices

The increased use of mobile devices that include full-featured internet browsers and downloadable applications has created a demand for parental controls on these devices. Some examples of mobile devices that contain parental controls include cell phones, tablets, and e-readers. In November 2007, Verizon was the first carrier to offer age-appropriate content filters and the first to offer generic content filters, recognizing that mobile devices were used to access all manner of content, from movies and music to short-code programs and websites. In June 2009, in iPhone OS 3.0, Apple was the first company to provide a built-in mechanism on mobile devices to create age brackets for users to block unwanted applications from being downloaded to the device. In the following years, all major operating systems developers have presented in-built tools for parental control, including Linux, Android, Windows, and even the more business-oriented platform, Blackberry. In addition, some applications allow parents to monitor real-time conversations on their children's phones via access to text messages, browser history, and application history.

An example of this is Trend Micro, which offers protection from viruses and parental controls to phones and tablets of almost all brands. Most of these offer the ability to add extra features to parental controls. These apps have the features mobile devices already have but have additional features such as monitoring and filtering texts/calls, protecting while surfing the web, and denying access to specific websites. Applications of this sort have created rising competition in their market.

Mobile device software enables parents to restrict which applications their child can access while also allowing parents to monitor text messages, phone logs, MMS pictures, and other transactions occurring on their child's mobile device; to enable parents to set a time limit on the usage of mobile devices, and to track the exact location of their children as well as monitor calls and the content of texts. This software also allows parents to monitor social media accounts. Parents can view posts, pictures, and any interactions in real-time. Another function of this software is to keep track of bullying. Most internet providers offer no-cost filtering options to limit internet browsing options and block unsuitable content. Implementing parental controls and discussing internet safety are useful steps to protect children from inappropriate information.

Although parental controls can protect children, they also come with some negative factors. For example, children's anxiety may increase due to parental controls. In extreme cases, a child may become so angry that they destroy their device, defeating the purpose of parental controls entirely. In that case, it might be a better idea to forgo installing parental controls.