

Service description of the secure browsing add-on service

General

The secure browsing add-on service is a subscription add-on service that allows for secure web browsing. It prevents you from visiting malicious sites where you could end up falling victim to phishing or malware, for example. The secure browsing add-on service works on DNA's mobile and fixed networks and does not require a separate installation on the user's device, thus not consuming the memory or capacity of the device used for browsing. On a mobile network, the secure browsing add-on service will keep your subscription secure even when you are abroad. The secure browsing add-on service is a subscription-specific service that covers the security of browsing through the connection on that subscription. The secure browsing add-on service is available for certain phone and broadband subscriptions.

Service deployment and deactivation

The secure browsing add-on service can be activated when you purchase a subscription. You can also activate the secure browsing add-on service for your subscription later on your own in the My DNA application or through DNA customer service. Access to pages identified as malicious will be blocked when the add-on service is active.

If necessary, you can turn off the secure browsing add-on service in My DNA or through customer service, so that access to harmful sites is no longer restricted.

When using a mobile connection, you need to turn on the aeroplane mode or restart the device for the service change to take effect immediately.

When using a fixed-network connection, you need to power off and power on the modem or router after the service is activated so that the service change will take immediate effect. If you do not restart the device, the change will take effect with a delay, but no later than on the next day.

Limitations of the secure browsing add-on service

The secure browsing add-on service blocks malicious sites identified by the service. The list of malicious sites is constantly updated, but the service cannot guarantee that all malicious sites have been identified and can be blocked. It is the customer's responsibility to exercise discretion and care when using the internet. DNA is not liable for any resulting damage caused to the customer.

The secure browsing add-on service may not be able to detect and block web pages that open in application-internal browsers. Depending on the browser or search engine or endpoint device settings, image and video search results from search engines may show harmful content, but the user is prevented from going to the sites.

If the website is https encrypted, the filtering of harmful content will work, and instead of seeing the service's own message, you will see an error message from the browser.

The secure browsing add-on service works on DNA's mobile network and fixed network. If, for example, you connect to the Wi-Fi network at a café or in another public place, the service will not filter out harmful

pages. When you use mobile broadband as your home internet connection, the secure browsing add-on service will protect the web browsing of all devices using that internet connection.

In order for the product to work, the customer must use the name server (DNS) addresses provided by DNA. Please note that your device and security applications may have features that allow for the encryption of outgoing network traffic using a proxy server. Such settings may include a separate DNS server in your browser, hiding your IP address or using the VPN feature. When these features are active, the secure browsing add-on service will not protect traffic, and filtering of malicious pages may not work.

Pricing of the secure browsing add-on service

The secure browsing add-on service is a free add-on service included with certain subscriptions. Activating and deactivating the service in the My DNA application or through customer service is free of charge.

Processing of personal data

The data are processed for the purpose of providing the secure browsing add-on service. The service processes information about the web addresses (URLs) classified as malicious that the connection has attempted to open. Otherwise, the secure browsing add-on service does not collect any information about the services used or websites visited with the subscription or device. Further information on the processing of personal data can be found in DNA's privacy policy.

Miscellaneous terms and conditions

For the parts not covered by the service description of the secure browsing add-on service, the currently valid DNA's General Terms and Conditions for Consumer Customers and the Special Terms and Conditions for Mobile Subscriptions for DNA's Consumer Customers apply.

