The growing economic importance of Global Navigation Satellite Systems (GNSS) makes it rewarding for malevolent people to aim at misleading receivers in their position and time estimation. This can be achieved by replacing or superposing signals to the authentic GNSS satellite signals and is called spoofing. Most current receivers are not designed to detect spoofing. The present article aims at a systematic exposition of threats. In many cases, they can be addressed by comparing the received signals, the estimated states, and their respective dynamics against models. A cryptographic signature of the navigation message would furthermore improve the detectability of fake synthetic signals, and should be implemented in the definition of new GNSS signals. In general, the analysis of spoofing should receive the same attention as the analysis of natural impairments. We hope that the present paper will contribute to achieve this.