and “Clickjacking”

Attackers can use clickjacking attacks to hijack Facebook accounts by tricking users into clicking on sites hiding malicious code. A Web site that looks like an e-commerce site or that shows videos could hide a Facebook log-in page behind it so that when a user clicks on the site to play a video, for instance, the user's account is opened instead behind the scenes, without the user realizing it.

Example of a clickjacking post:

If you're curious enough to click on the link, your browser will be taken to a webpage which pretends to be a YouTube-style video site called FbVideo.

If you've got this far, you'll probably be tempted to click to view the video. However, like the many clickjacking attacks we saw on Facebook last year, you will be invisibly clicking on a "Like" button without your knowledge, sharing the link further with your friends

The page is designed to display a survey scam, which both earns money for the scammers and can trick you into handing over your mobile phone number to sign you up for a premium rate SMS service.

Other versions of the scam:

If you find you have accidentally "Liked" an offending webpage, remove references to it from your wall and check your profile settings.

Itmakes sense to logout from Facebook when you are not actively using it to reduce the chances of you being tricked into "Liking" things you don't really like.