ინტერნეტ ბრაუზერების უსაფრთხოდ გამოყენება

თითქმის ყველა კომპიუტერზე დაყენებულია ვებ-ბრაუზერი (Internet Explorer, Opera, Chrome, Mozilla Firefox, Apple Safari). ვინაიდან ვებ ბრაუზერები განსაკუთრებით ხშირად გამოიყენება, საჭიროა მათი კონფიგურირება უსაფრთხოების მოთხოვნების შესაბამისად. ხშირად ახლად დაყენებული ვებ-ბრაუზერებში არ არის გააქტიურებული უსაფრთხოების საშუალებები და ფუნქციები. დაუცველი ბრაუზერის მეშვეობით შესაძლებელია, პერსონალური მონაცემების დაკარგვა, კომპიუტერის დაინფიცირება, დაზიანება და ა.შ.

ხშირად კომპიუტერები იყიდება წინასწარ ჩაწერილი პროგრამული უზრუნველყოფით. ასეთ შემთხვევაში აუცილებელია კომპიუტერის ახალმა მფლობელმა პირველ რიგში შეამოწმოს რა პროგრამებია დაინსტალირებული კომპიუტერში, შემდეგ განიხილოს რამდენად ახალი და საბოლოო ვერსიებია დაყენებული, ასევე რამდენად გამართულია კონფიგურაცია უსაფრთხოების თავალსაზრისით. ვინაიდან ვებ-ბრაუზერები კიბერ-შეტევების ერთერთი უმთავრესი და ყველაზე გავრცელებული ვექტორია, საჭიროა მათი ფუნქციონირების მუდმივი მონიტორინგი.

კიბერ-შემტევები ამზადებენ სპეციალურად მოდიფიცირებულ ვებ გვერდებს, რომელთა მონახულებისას ინტერნეტ მომხმარებლის დაუცველი ვებ-ბრაუზერის მეშვეობით, ავტომატურად ინფიცირდება კომპიუტერული სისტემა.

არსებობს რამდენიმე ფაქტორი რაც ხელს უწყობს ვებ ბრაუზერით კომპიუტერის დაზიანება-დაინფიცირებას:

- ბევრი ინტერნეტ მომხმარებელი ხსნის უცნობ საიტებს და ლინკებს, რისკის გაცნობიერების გარეშე.
- ერთ ვებსაიტზე შესვლისას შესაძლებელია ავტომატურად ჩაიტვირთოს სხვა ვებსაიტზე განთავსებული მავნე კოდი.
- ვებ ბრაუზერები მომხმარებელს სთავაზობს გაზრდილ ფუნქციონალურობას, რის ხარჯზეც მცირდება, უსაფრთხოება.
- ყოველკვირეულად ხდება ახალი სისუსტეების აღმოჩენა სხვადასხვა ვებ ბრაუზერში და ინტერნეტ დაპროგრამების ტექნოლოგიებში. მათი თავდაცვის მექანიზმების შემუშავებას კი ზოგჯერ თვეები სჭირდება.

- კომპიუტერულ სისტემებს და ზოგიერთ ვებ-ბრაუზერს შეიძლება თან ახლდეს სხვა უცხო პროგრამული პროდუქტი, რომლის სისუსტეზე ზემოქმედებით შესაძლებელია მთალიანი კომპიუტერის ინფიცირება და მომხარებლის პრივატული ინფორმაციის ხელში ჩაგდება.
- ხშირად მომხმარებლებს გათიშული აქვთ ავტომატური განახლებების ფუნქციები.
- ასევე მრავალმა ინტერნეტ მომხმარებელმა არ იცის ინტერნეტ საფრთხეების შესახებ და ზოგჯერ არც სურს თავდაცვის მექანიზმების გამოყენება.

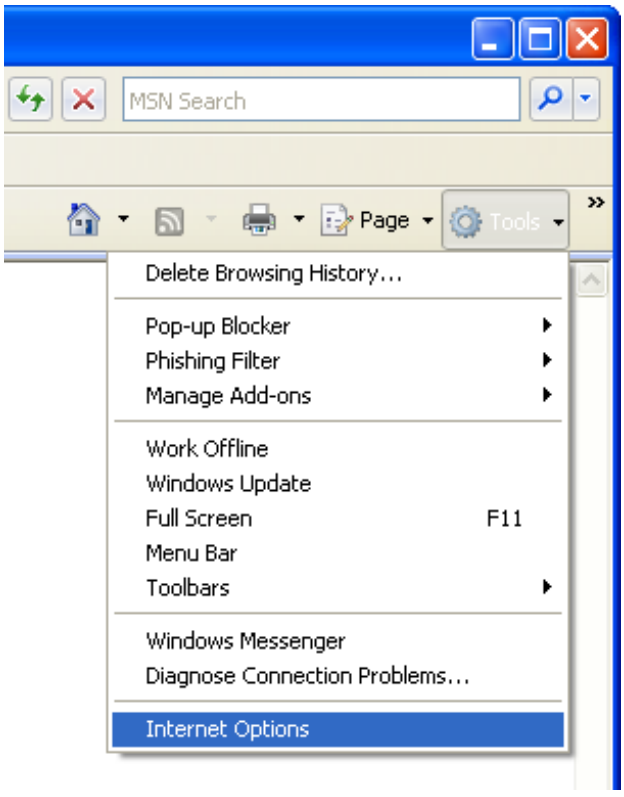
ბრაუზერის უსაფრთხოების გამართვის წესები

ქვემოთ მოყვანილია რამდენიმე პოპულარული ვებ-ბრაუზერის კონფიგურირების ინსტრუქციები, რის შედეგადაც საგრძნობლად შემცირდება ინტერნეტ საფრთხეები და შესაბამისი რისკები.

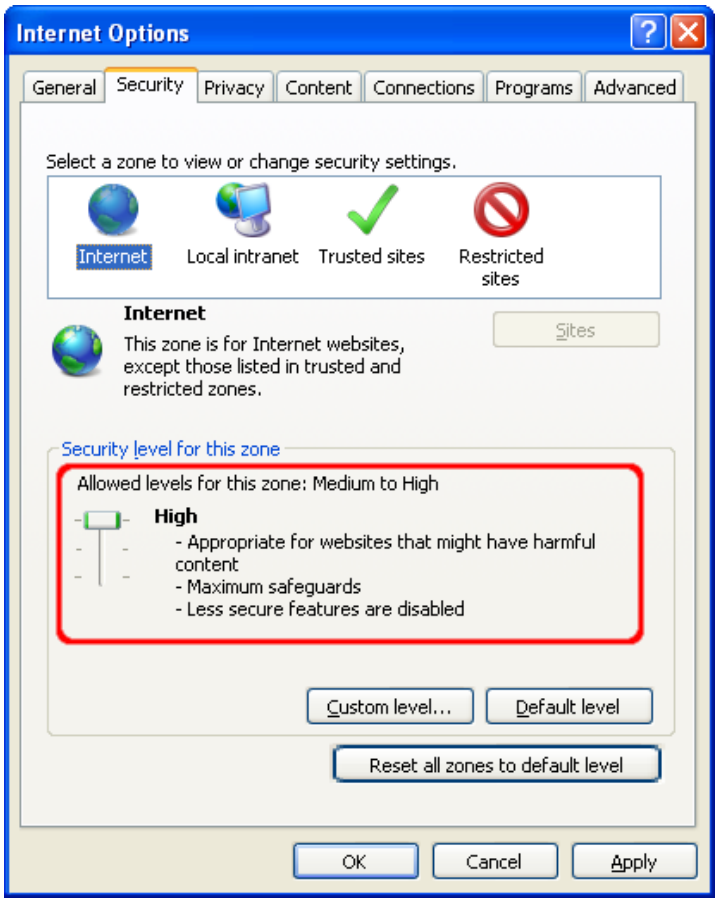
Microsoft Internet Explorer - ეს ვებ ბრაუზერი ინტეგრირებულია ოპერაციულ სისტემა Windows-ში. ამიტომ ბევრი Windows ინტერნეტ მომხმარებელი სწორედ ამ ბრაუზერს იყენებს.

პარამეტრების შესაცვლელად საჭიროა შემდეგი მოქმედებების შესრულება (საგულისხმოა რომ, მენიუს ტიპი და შემადგენლობა შეიძლება იცვლებოდეს პროგრამის ვერსიის მიხედვით)

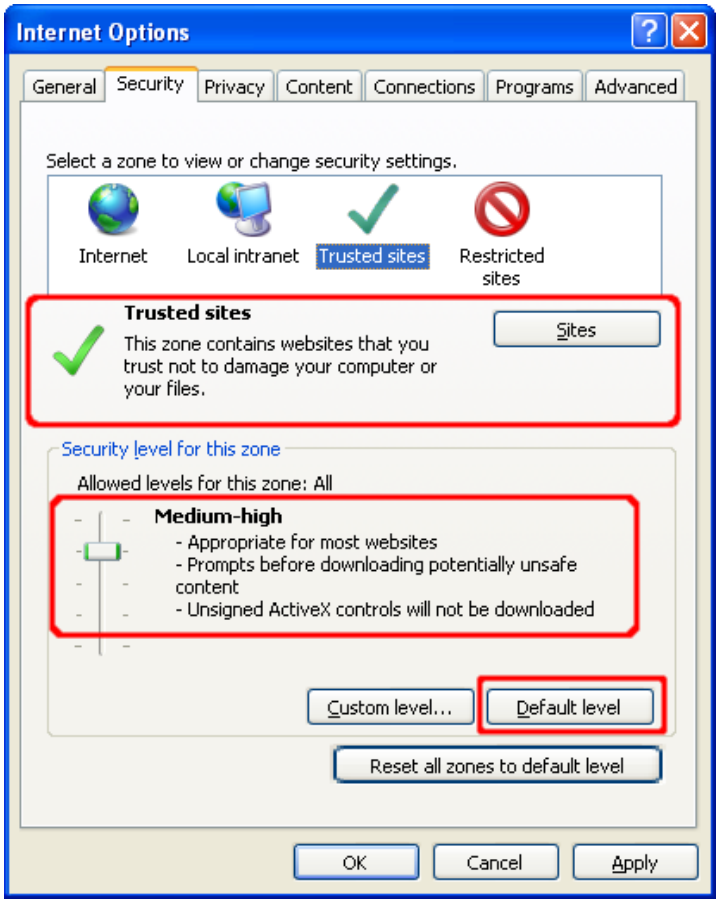
1) Tools -> Internet Options



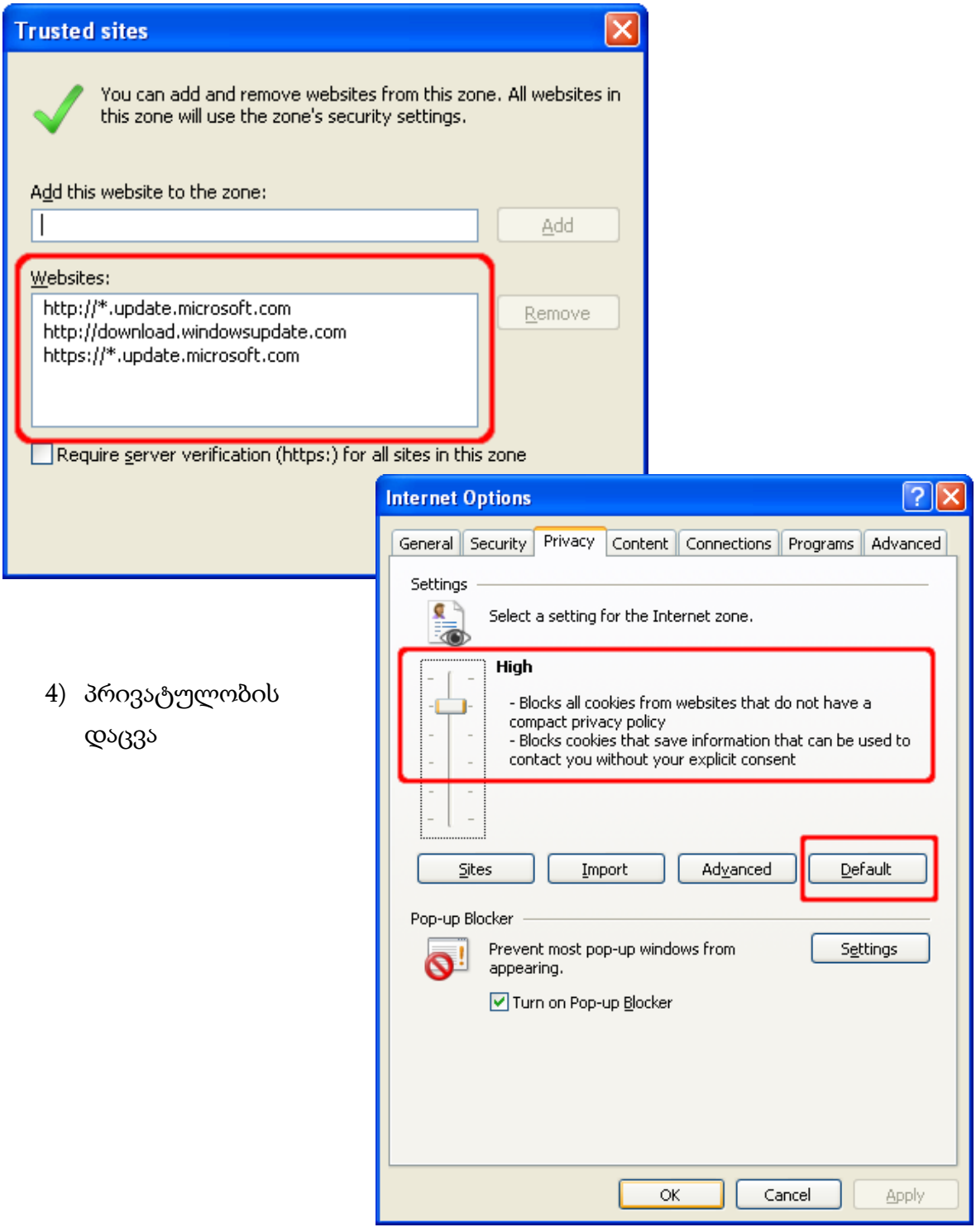
2) Security Tab



3) საშუალო დონის უსაფრთხოება

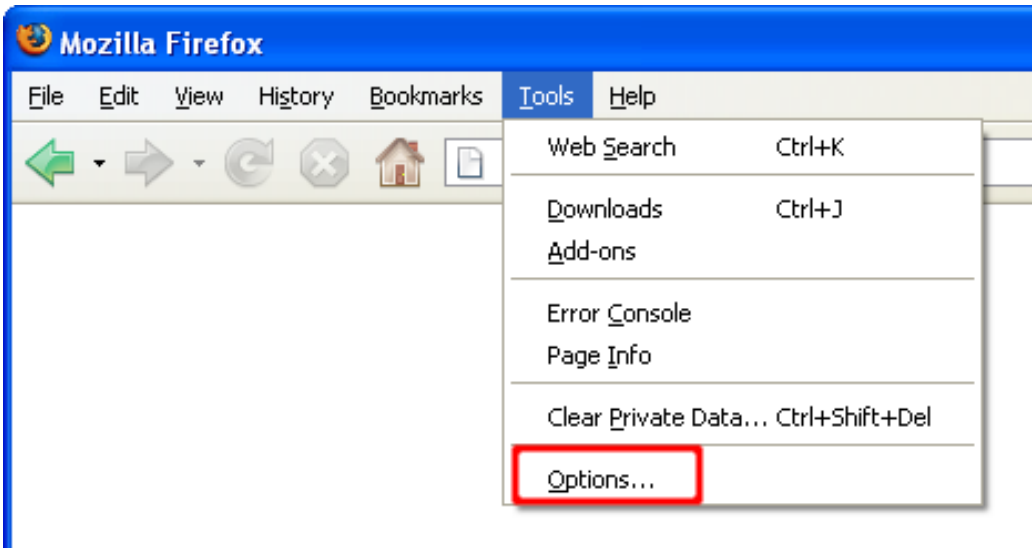


ამ შემთხვევაში შესაძლებელია სანდო საიტების ჩამატება, სადაც არ იქნება გამოყენებული მკაცრი კონტროლის მექანიზმები:

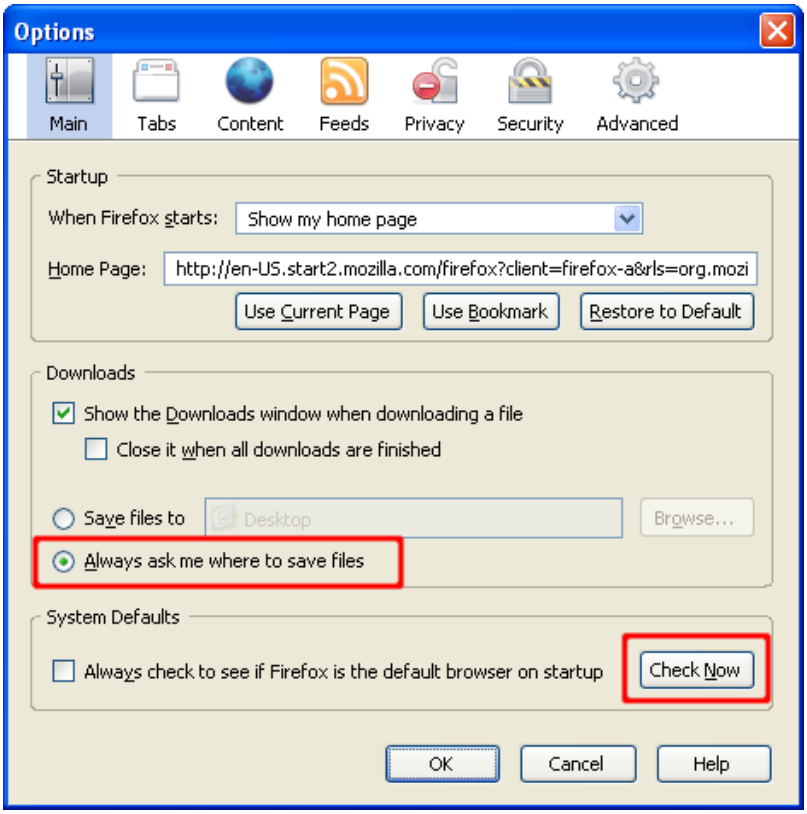


4) პრივატულობის დაცვა

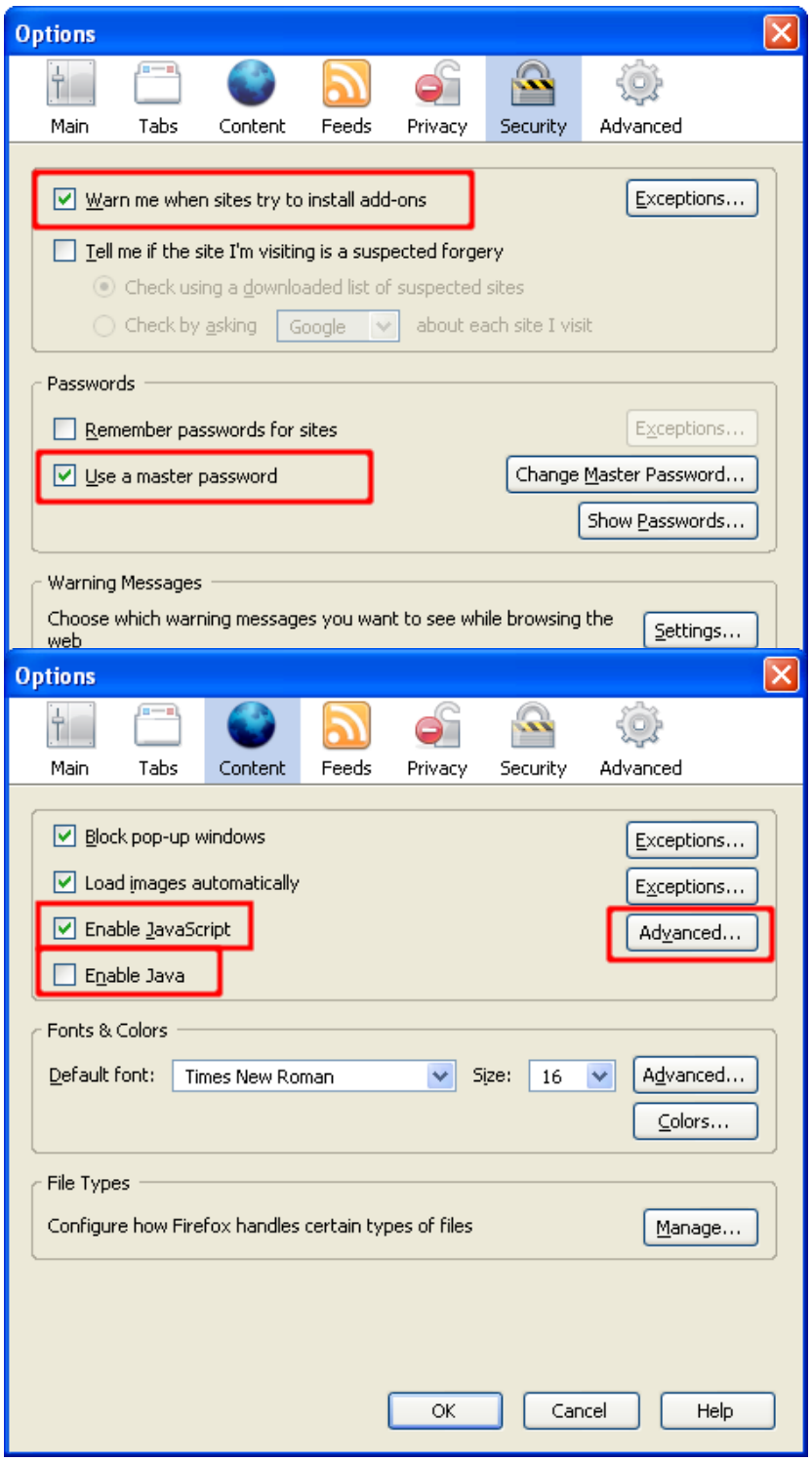
Mozilla Firefox



1) ფაილების ავტომატურად შენახვის ფუნქციის გათიშვა

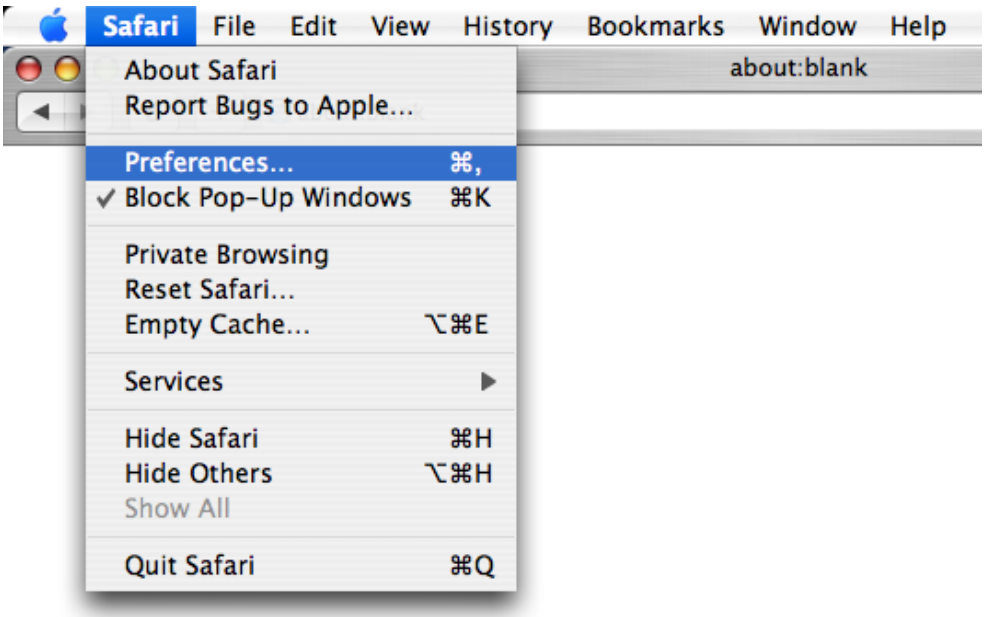


2) არასასურველი დამატებების დაყენების პრევენცია

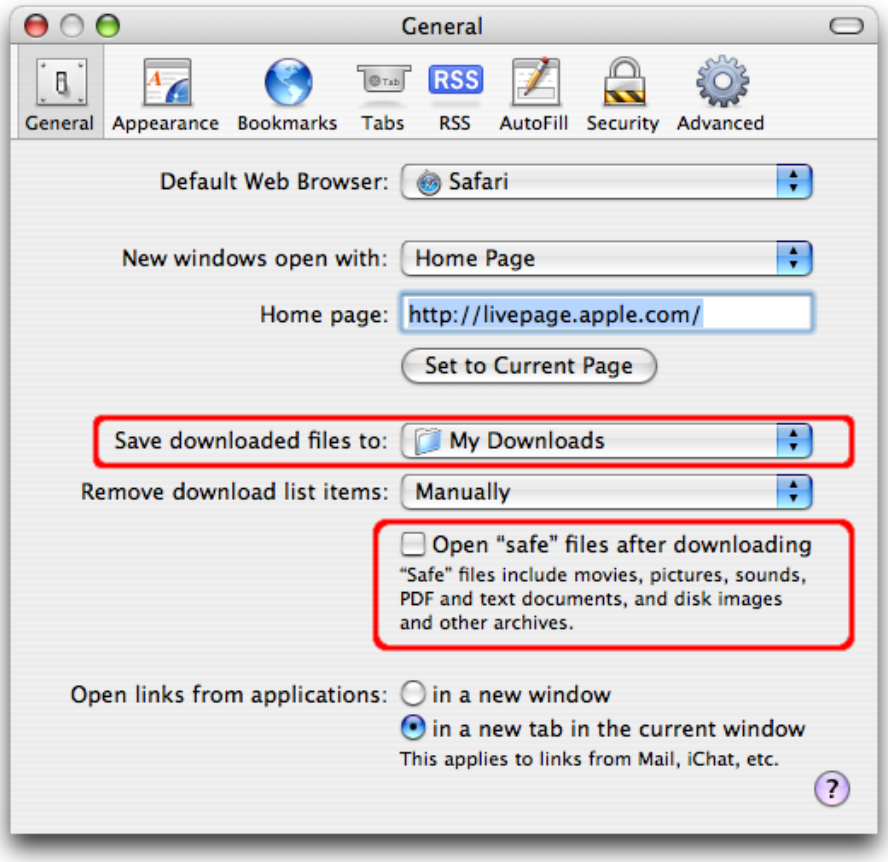


3) სახიფათო შიგთავსის გამოყენების კონფიგურირება

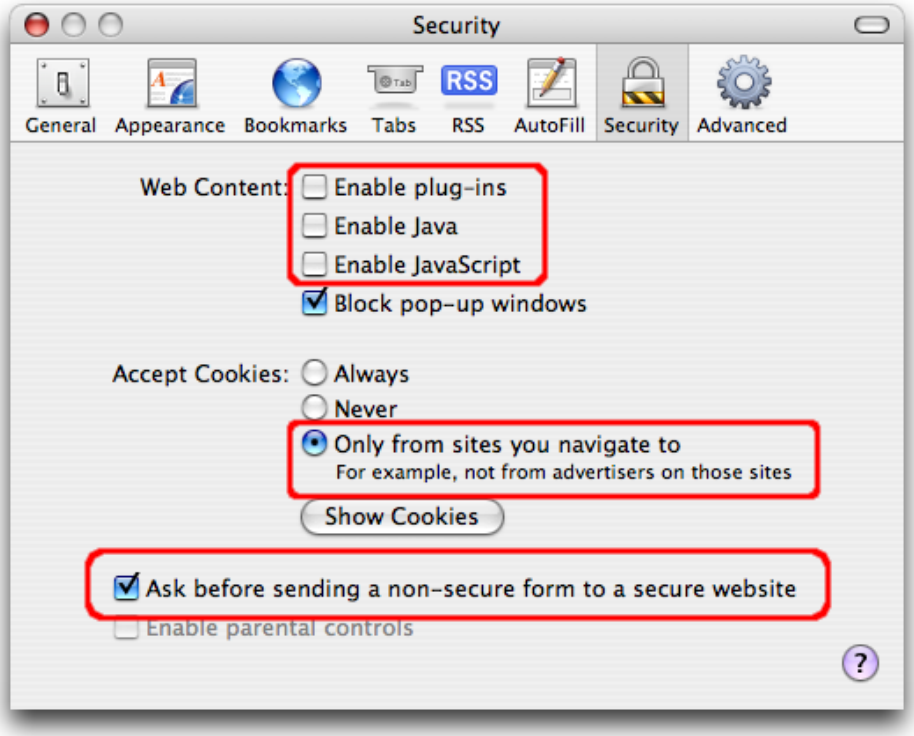
Apple Safari



1) ფაილების ავტომატურად გადმოწერის და გაშვების ფუნქციის გათიშვა



2) სახიფათო კონტენტის, საიტებზე არსებული პოტენციური მავნე კოდებისგან თავის დაცვა


Security
General
Appearance
Bookmarks
Tabs
RSS
AutoFill
Security
Advanced
Web Content:
Enable plug-ins
Enable Java
Enable JavaScript
Block pop-up windows
Accept Cookies:
Always
Never
Only from sites you navigate to
For example, not from advertisers on those sites
Show Cookies
Ask before sending a non-secure form to a secure website
Enable parental controls