**ლექცია № 7 ბრაუზერების უსაფრთხოება.**

დღესდღეობით ბრაუზერები უკვე აღარ არიან მხოლოდ html კოდის ამსახველი საშუალე­ბები, ისინი გადაიქცნენ ”თითქმის ყველაფრათ”. ისინი არიან ასევე სათამაშო სადგური, რაც ითხოვს დიდი რაოდენობის სკრიპტების (**სკრიპტი** (Script) - ანუ სცენარი, არის ბრძანებების - ოპარატორების კრებული რომელიც შემდეგ სრულდება რაიმე პროგრამის მიერ, მაგალითად Javascript არის HTML გვერდში ჩატანებული თავისებული პროგრამული კოდი. სკრიპტის კომპილირება არ ხდება, იგი რეალიზდება ინტერპრეტატორის საშუალებით, მათ შორის ბრაუზერით) და მედიასტუდიების მხარდაჭერას. ეს უკანასკნელი კი მიიღწევა თავის მხრივ **პლაგინების** (*plug-in*, *plug in* -სიტყვა ჩართვა-დან, დამოუკიდებლად კომპილირებადი პროგრამული მოდული, რომელიც ძირითად პროგრამას დინამიურად მიუერთდება და იწვევს მისი შესაძლებლობების გაფართოებას) მხარდაჭერით. სწორედ სკრიპრები და პლაგინები წარმოადგენენ ბრაუზერების ყველაზე უფრო მოწყვლად ნაწილებს. კერძოდ ზიანისმომტან პროგრამებს შეუძლიათ ისარგებლონ ბრაუზერის შესაძლებლობებით მხარი დაუჭიროს:

***სკრიპტებს***: პროგრამული კოდის ეს მცირე ელემენტები, დაწერილია JavaScript ან VisualBasic ენებზე. ზიანისმომტანი სკრიპტები, როგორც წესი, ფარულად ჩაწერენ ვირუსებს კომპიუტერში, უშუალოდ ”აწყობენ” დაავადებულ კომპიუტერზე ზიანისმომტან პროგრამებს, ან არასანქცირებულად გადაამისამართებენ სულ სხვა საიტზე;

**უჩინარ ფანჯრებს** ( inline frame, შემოკლებით IFRAME) iframe - ეს ჩვეულებრივი html ტეგია, რომელიც უჩინარ ფანჯარას ქმნის, რომლის დაკეტვა( დახურვა) შეუძლებელია ჩვეულებრივი გზით. მათი საშუალებით ხდება ბანერული რეკლამის ჩვენება, ხოლო მისი ზიანისმომტანი ხასიათი ჩნდება მაშინ, როცა მას შეუძლია გადაამისამართოს მომხმარებელი დაინფიცირებულ საიტზე, იმ სკრიპტის საშუალებით, რომელიც ამ ტეგის შიგნითაა მოთავსებული. ბრაუზერებში შესაძლებელია iframe ტეგის დამუშავების გამორთვა.

**ActiveX ელემენტებს.** ( ActiveX - ეს Microsoft OLE 2.0 ტექნოლოგიაა. ტექნოლოგია ActiveX ძირითადათ გამოიყენაბა იმისთვის, რომ ვებ-გვერდზე ჩაირთოს მულტიმედია-მონაცემები) თუ კი დაშვებულია ActiveX -ის ელემენტების მართვა, ისინი შეიძლება დაყენებულ იქნან კომპიუტერზე უშუალოდ საიტიდან, რაც უზრუნველყოფს უფრო ინტენსიურ ურთიერთქმედებას კომპიურეტსა და სერვერს შორის. თუ კი ეს ელემენტი ზიანისმომტანის, მას შეუძლია დიდი ზიანის მოყენება. თუ კი ActiveX ელემენტის დაყენების აუცილებლობა არ არის, მაშინ ჯობს იგი იყოს გამორთული.

**გარეშე დეველოპერების (პროგრამისტების, შემმუშაველების) პლაგინებს.** ზოგჯერ პლაგინში შეიძლება ჩართული იყოს რაიმე ჯაშუშური მოდული ან/და პროგრამა ტროიანი. მთელი საშიშროება იმაშია, რომ თუ კი ზიანისმომტანი პროგრამა ბრაუზერში მოხვდა, მაშინ ბრანდმაუერი კარგავს კონტროლს ქსელზე. ჩვეულებრივ ბარაუზერს აქვს სრული წვდომა ქსელში, შესაბამისად პლაგინ-ტროანელსაც ან ჯაშუშს.

განვიხილოთ ზოგიერთი ბრაუზერების უსაფრთხოების ამაღლების მეთოდები.

**Internet Explorer**

**უსაფრთხოების ზონები**

უსაფრთხოების ზონები წარმოადგენს ინტერნეტის მომხმარებელთა თავდაცვის ძირითად საშუალებას. გაჩუმების პრინციპით ყველა ვებ-საიტი მიეკუთვნება ინტერნეტის ზონას, ხოლო **Internet Explorer** -ი მკაცრად განსაზღვრავს მოქმედებათა სახეებს ამა თუ იმ ზონის ვებ-საიტებისათვის. კერძოდ, არსებობს უსაფრთხოების ოთხი ზონა:

- ლოკალური ინტრაქსელი (**Local Intranet**). ეს ზონა განკუთვნილია ვებ-საიტების განსათავსებლად ორგანიზაციის შიგნით;

- სანდო ვებ-საიტები (**Trusted Sites**). ამ საიტებს ენიჭებათ ნდობის უმაღლესი დონე. (მაგალითად, ვებ-საიტები თქვენი საქმიანი პარტნიორებისათვის);



ნახატი 1.

- შეზღუდული ვებ-საიტები (**Restricted Sites zone**). ესაა საიტები, რომლებსაც დანამდვილე­ბით არ ენდობით.

- ინტერნეტი (**Internet Zone**). ეს ზონა განკუთვნილია იმ ვებ-საიტებისათვის, რომლებიც არ მოხვდნენ არც ერთ წინა კატეგორიაში.

უსაფრთხოების ზონების კონფიგურირებისათვის შეასრულეთ შემდეგი ბრძანებები: **Tools » Internet Options » Security** იხ.ნახ.1.

ვებ-საიტის ზონაში ჩასამატებლად აირჩიეთ ზემოჩამოთვლილი ზონიდან ერთ-ერთი და ველში **Add this Web site to the zone**, აკრიფეთ ვებ-საიტის URL -ლინკი და დააჭირეთ ღილაკს OK. იხ.ნახ.2.



ნახატი 2

ოფცია **Require server verification (https:) for all sites in this zone** (ამ ზონის ყველა კვანძისათვის აუცილებელია (https:) სერვერების შემოწმება. თუ საჭიროა ისეთი ვებ-საიტის ჩამატება, რომელიც არ იყენებს HTTPS პროტოკოლს, საკმარისია ალამის გამორთვა.