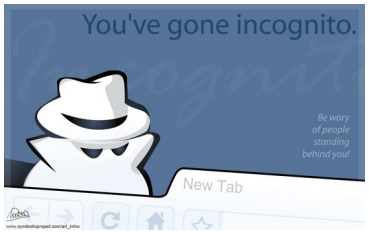
Browser Basics

Saved Passwords/AutoFill Data: It is recommended you never save passwords or any personal information in browsers due to the fact that browsers don't encrypted information. So this information can be retrieved by hackers using very basic tools. . Remove any passwords or confidential information already saved.

Pop-Up Blockers: Pop-up advertisements can present numerous security vulnerabilities. Be sure you only allow pop-ups on trusted sites.

JavaScript: While JavaScript is not inherently bad, it is notorious for containing security vulnerabilities. Only enable it for trusted sites.

Private Browsing: Almost every browser now has a form of “Safe” or “Private” browsing. This usually means that browsing history and cookie data are deleted once you quit the browser. Be aware that any files you save and bookmarks you add will still remain.



Additional Information

For a full write-up and image walk-throughs, please visit the IT Security Website:

http://security.vpit.txstate.edu/browsers/

Resources

Chrome’s Privacy Settings:
http://ow.ly/AhJi8

Firefox’s Security and Password Settings:
http://ow.ly/AhJaP

Security and Privacy Settings in IE 11:
http://ow.ly/AhIYu

Safari 6 Security Preferences:
http://ow.ly/AhJm2

This information is available in alternate format upon request from the Office of Disability Services.

Fall 2015

Texas State
INFORMATION TECHNOLOGY

IT Security

Web Browser Security Tips

512.245.4225
itsecurity@txstate.edu
Security.vpit.txstate.edu

Texas State University
A member of The Texas State University System

Mozilla Firefox

These settings can be accessed by typing **about:preferences** on the address bar.

Preferences

Privacy
Select → Use custom settings for history
Deselect → Remember my browsing and download history
Deselect → Remember search and form history
Deselect → Accept third-party cookies
Select → Keep until I close Firefox
Select → Clear history when Firefox closes

Security
Select → Warn me when sites try to install add-ons
Select → Block reported attack sites
Select → Block reported web forgeries
Deselect → Remember passwords for sites

Content
Select → Block pop-up windows
turn on automatic updates.

Google Chrome

These settings can be accessed by typing **chrome://settings/** on the address bar

Show advanced settings

Privacy
Passwords and forms settings:
Deselect → Offer to save passwords I enter on the web
Deselect → Offer to save your web passwords

Content Settings
Cookies
Select → Keep local data only until I quit my browser
Select → Block third-party cookies and site data

JavaScript
Select → Do not allow any site to run JavaScript

Pop-ups
Select → Do not allow site to show pop-ups

Location
Select → Do not allow any site to track your physical location

Media
Select → Do not allow site to access your camera and microphone

Unsandboxed plugin access
Select → Do not allow any sites to use a plugin to access your computer

Automatic Downloads
Select → Ask when a site tries to download files automatically after the first file

Safari

These settings can be accessed under Safari, Preferences...

Security
Select → Warn when visiting a fraudulent website
Deselect → Enable JavaScript
Select → Block pop-up windows
Deselect → Allow Plug-ins

Privacy
Cookies and website data:
Select → Always block

Website use of location services:
Select → Deny without prompting

Internet Explorer

These settings can be accessed through the “Internet Options” menu.

Privacy Settings
Select → Medium High or higher.
Select → Never allow websites to request your physical location.
Select → Turn on Pop-up Blocker

General
Select → Delete browsing history on exit

Security
Set security zones to your desired level
Select → Trusted Sites
Select → Enable Protected Mode

Content
Select → Delect AutoComplete History