



State of New Hampshire

Department of Safety

Division of Fire Standards and Training and Emergency Medical Services
Richard M. Flynn Fire Academy
98 Smokey Bear Blvd., Concord, New Hampshire
Mailing Address: 33 Hazen Drive, Concord, New Hampshire 03305-0002



John J. Barthelmes
Commissioner

Richard A. Mason
Director

MEMORANDUM

TO: NH EMS Units
NH EMS Regional Chairs
NH EMS Hospital Coordinators

FROM: Michael Schnyder, BS, SSBB, NREMT-P
FST & EMS
Bureau of EMS

RE: Verifying Optimal Security Setting for Your Internet Browsers

DATE: April 14, 2008

On behalf of the New Hampshire Department of Safety, Division of Fire Standards and Training and Emergency Medical Services (FST & EMS), we would like to take this opportunity to notify you about updating your TEMSIS security settings.

The majority of the Trauma and EMS Information System (TEMSIS) users create patient care reports using the Internet-based solution. Quite recently a number of news events have come into the light about the diligence required to protect private information. After an expedited review of TEMSIS' practices, we requested our software vendor, ImageTrend, to develop a "best practices" document on Internet Browser settings.

We now ask for each EMS or Fire agency, hospital, and anyone who uses TEMSIS to set their Internet Browsers to the maximal level to protect against potential threats. To assist everyone with this process, we took ImageTrend's work and divided it into three components:

- Best Practices for Microsoft Internet Explorer
- Best Practices for Mozilla Firefox
- An "expert level" document for those organizations with an established IT staff.

These documents will be located both on the TEMSIS (www.nhtemsis.org) and EMS Bureau's websites (<http://www.nh.gov/safety/divisions/fstems/ems/forms.html>).

Please also take the time to review your overall current security practices to ensure that protected health information (PHI) is at its the best. This ranges from the simple idea of not leaving a drop-off form on a counter to storing PHI in secure location.

If you have any questions about Internet browser security practices, please contact ImageTrend at: 1.888.469.7789. For other questions, please contact the Bureau's Research & Quality Management Section at 603-223-4226.

Fire Training – Certification – Fire Academy – Emergency Medical Services

Business: (603) 271-2661

Fax: (603) 271-1091

Toll Free: 1-800-371-4503

TDD Access: 1-800-735-2964

www.state.nh.us/safety/fst

Internet Browser Best Practices

Updating Your Security Settings For Internet Explorer

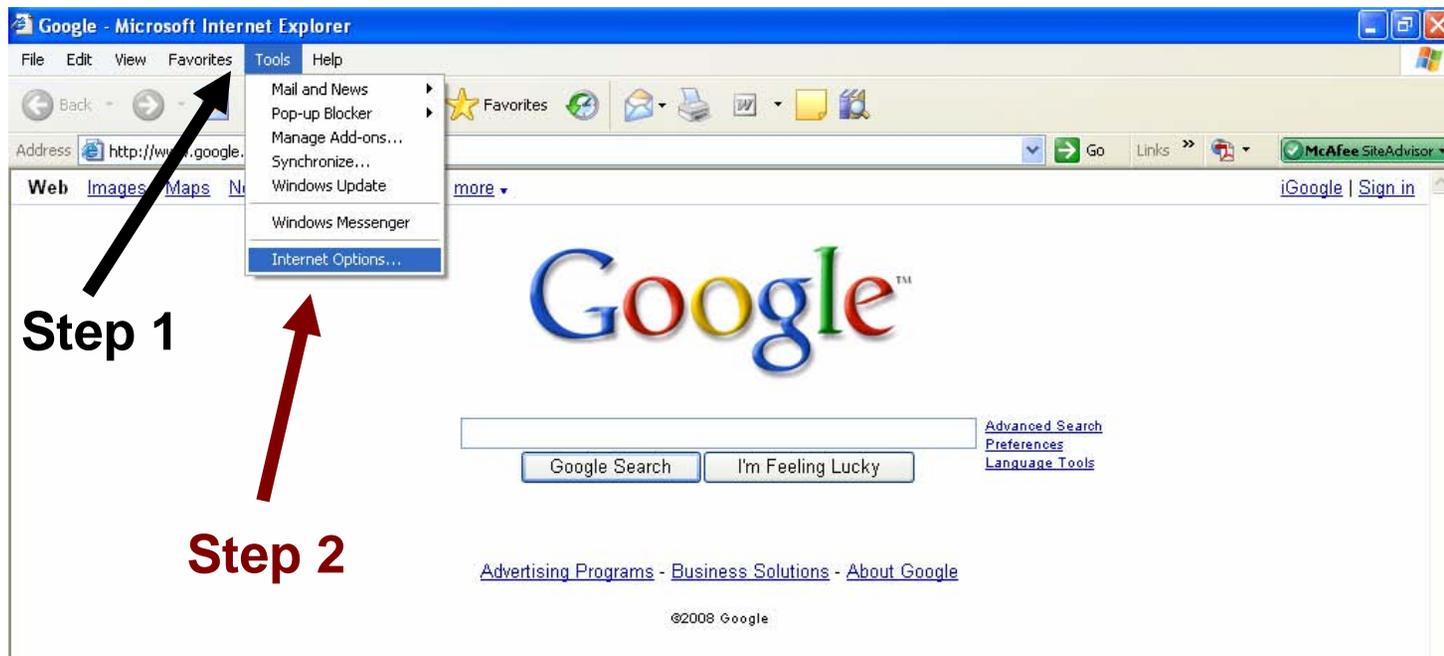
Introduction: Any computer that is or may be used to access patient data should conform to industry best practices standards for security.

Outlined in the following pages are simple changes to your Web browser recommended by ImageTrend that increase the level of protection of data, and improve the security on your computer.

These instructions were created using ImageTrend's
Internet Best Practices Document of 4/3/2008

Fundamental Microsoft Internet Explorer Configuration

The following recommendations are specific to Internet Explorer 7; however, previous versions of Internet Explorer should follow similar guidelines as much as possible.

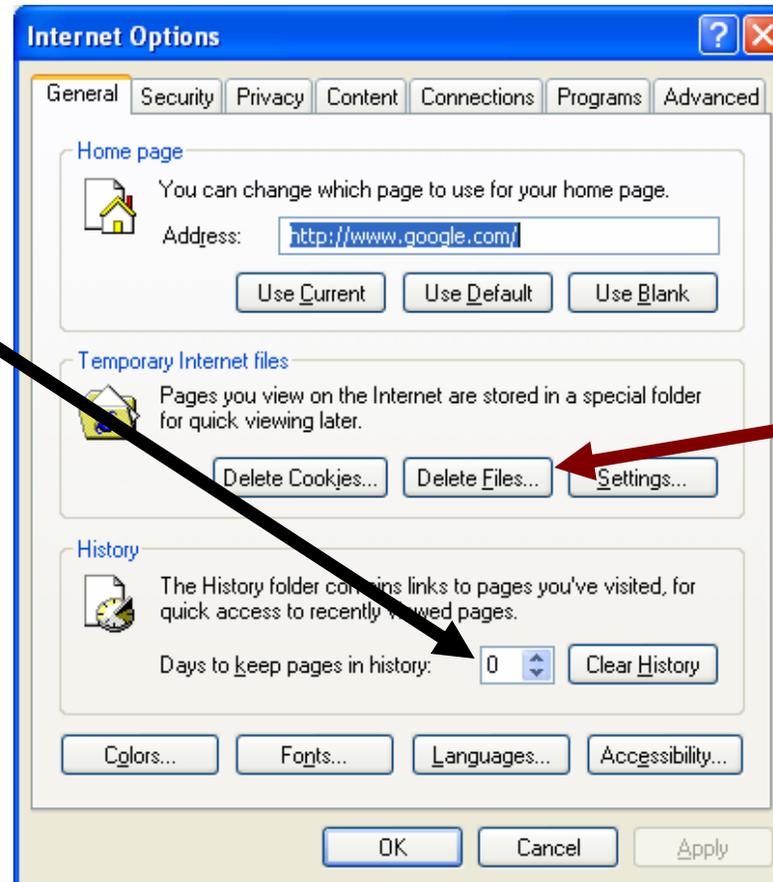


Step 1: Find the **Tools** section for your Internet Browser

Step 2: Next, find and click on the **Internet Options** link

Fundamental Microsoft Internet Explorer Configuration

Step 3

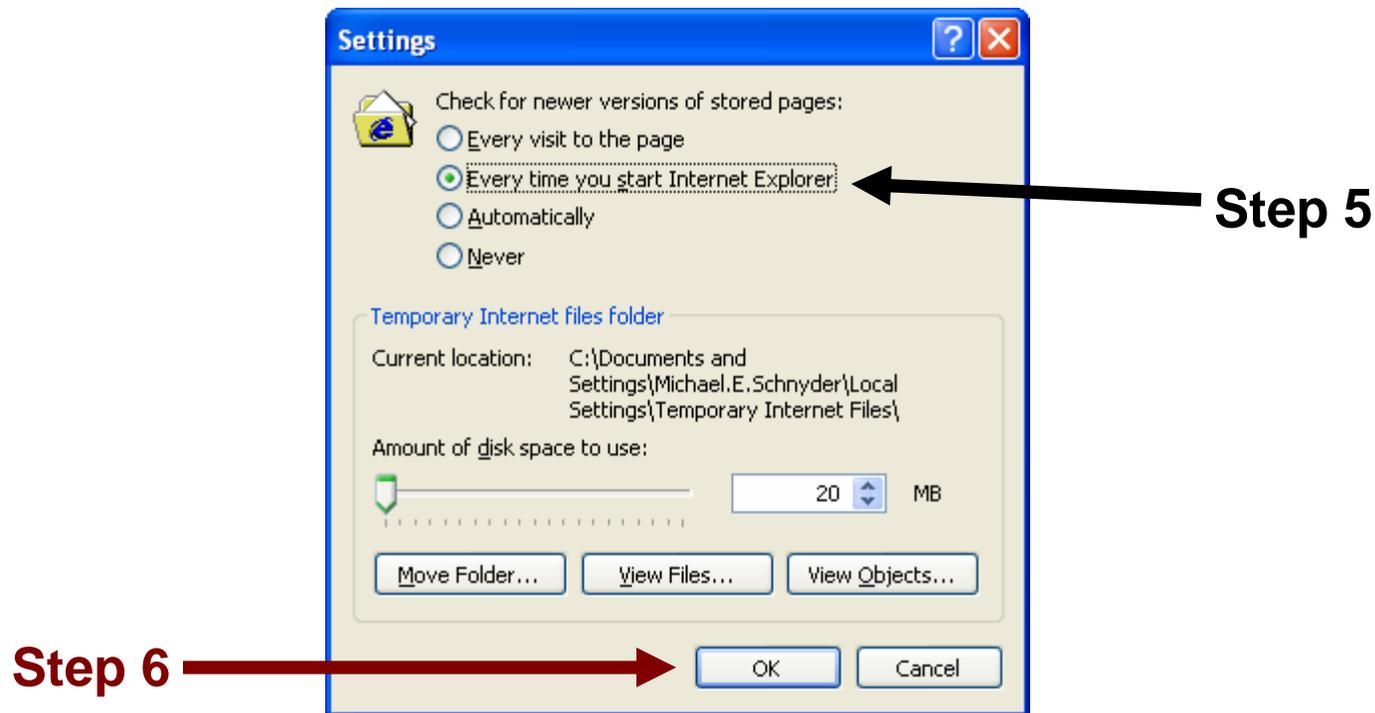


Step 4

Step 3: Set the number of days the History is kept to **0 (Zero)**

Step 4: Next, click on the **Settings** link

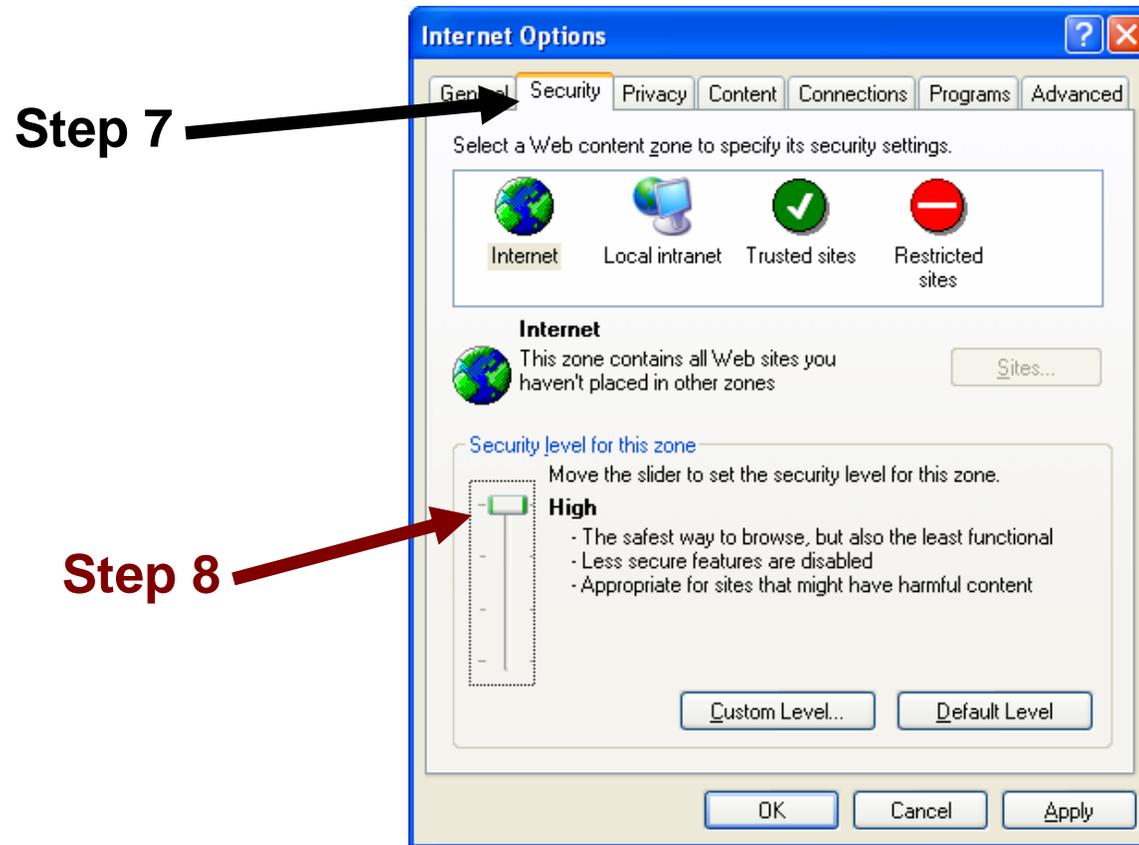
Fundamental Microsoft Internet Explorer Configuration



Step 5: Click the button that states **Every visit to the page** or **Every time you start Internet Explorer**

Step 6: Next, find and click on the **OK** button

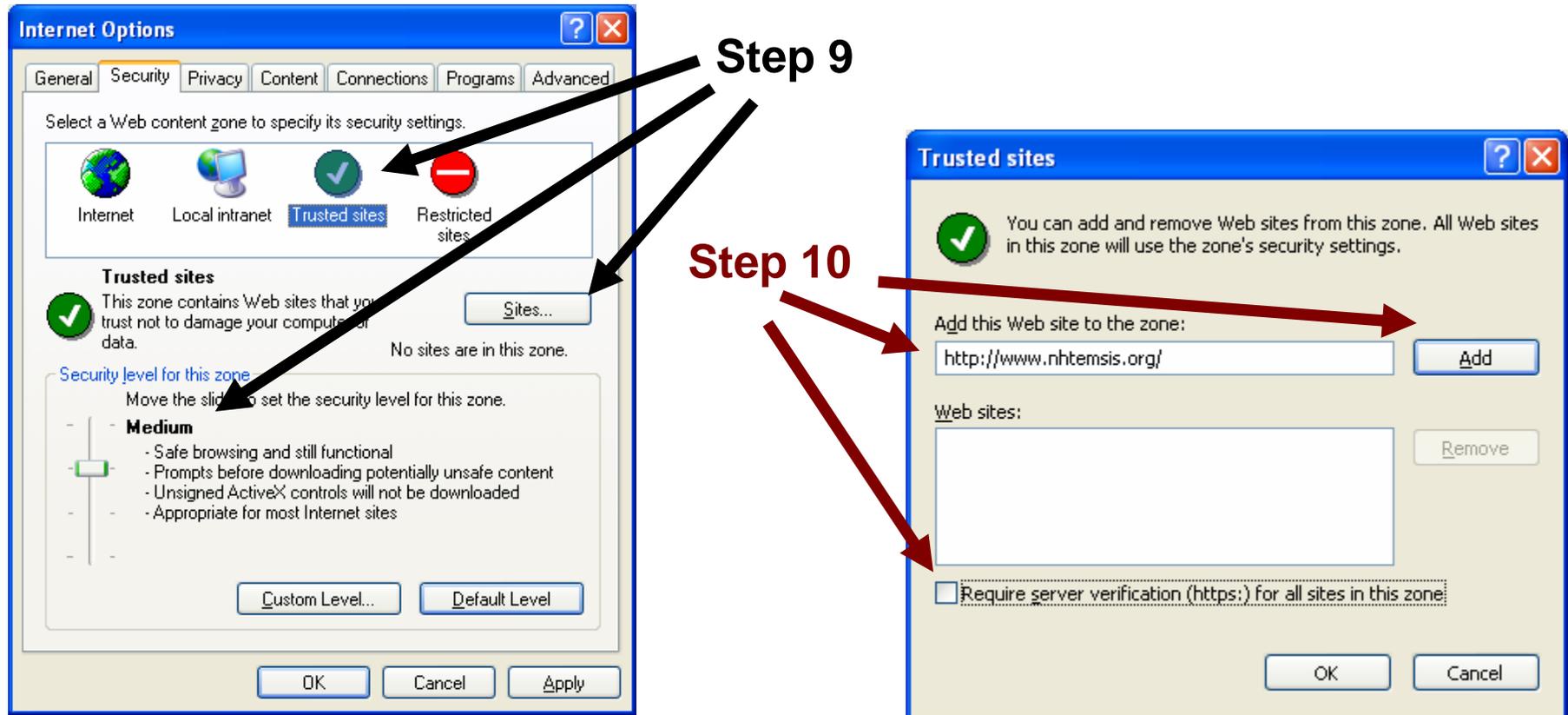
Fundamental Microsoft Internet Explorer Configuration



Step 7: Click on the **Security** tab

Step 8: Set your security levels to **HIGH**

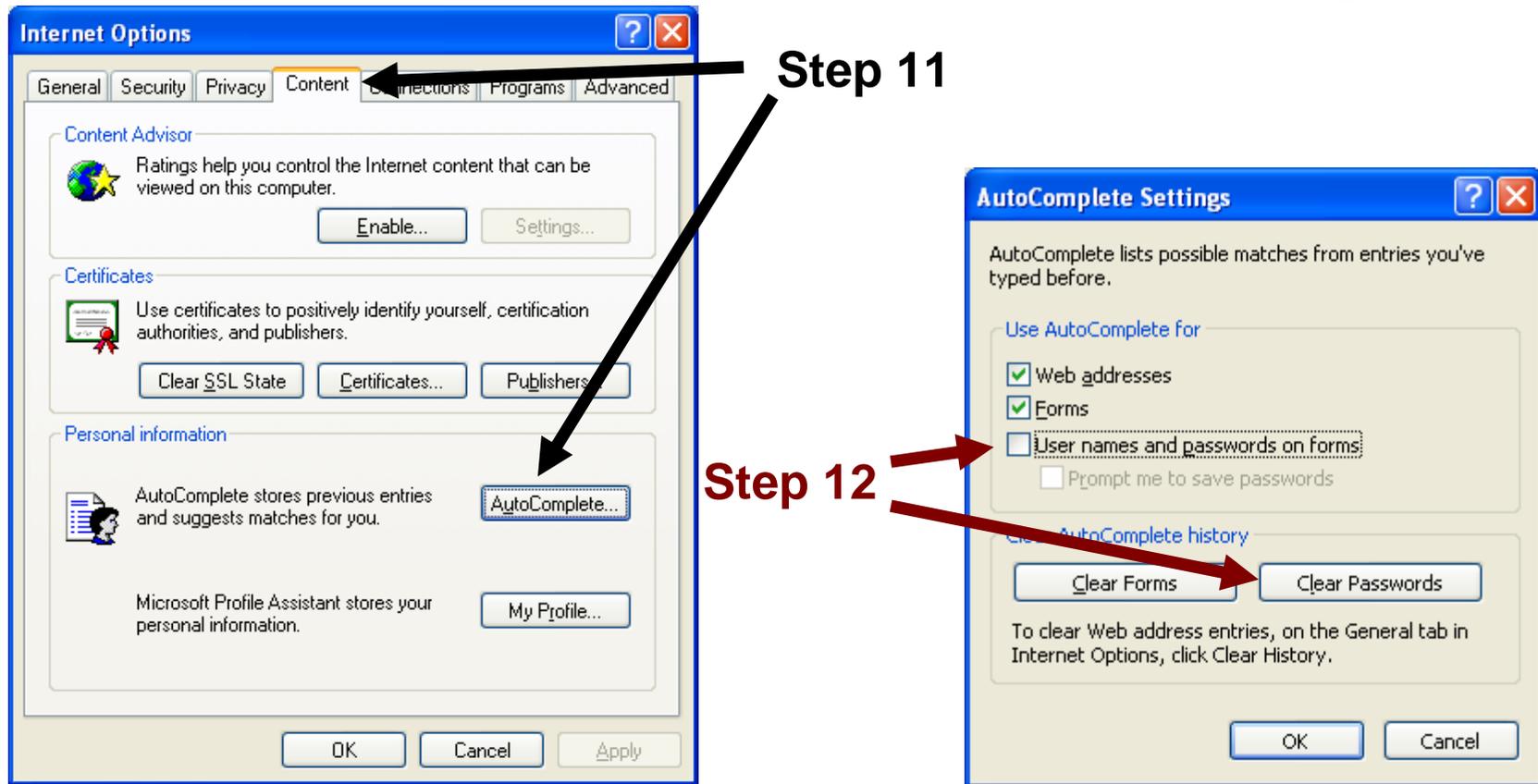
Fundamental Microsoft Internet Explorer Configuration



Step 9: Click on the **Trusted Sites** link. Make sure the Security Level is set to **Medium** for this section. Then click on the **Sites** link.

Step 10: Type in **http://www.nhtemsis.org/**, click **Add**, uncheck **Require Server** box, and then click the **OK** button

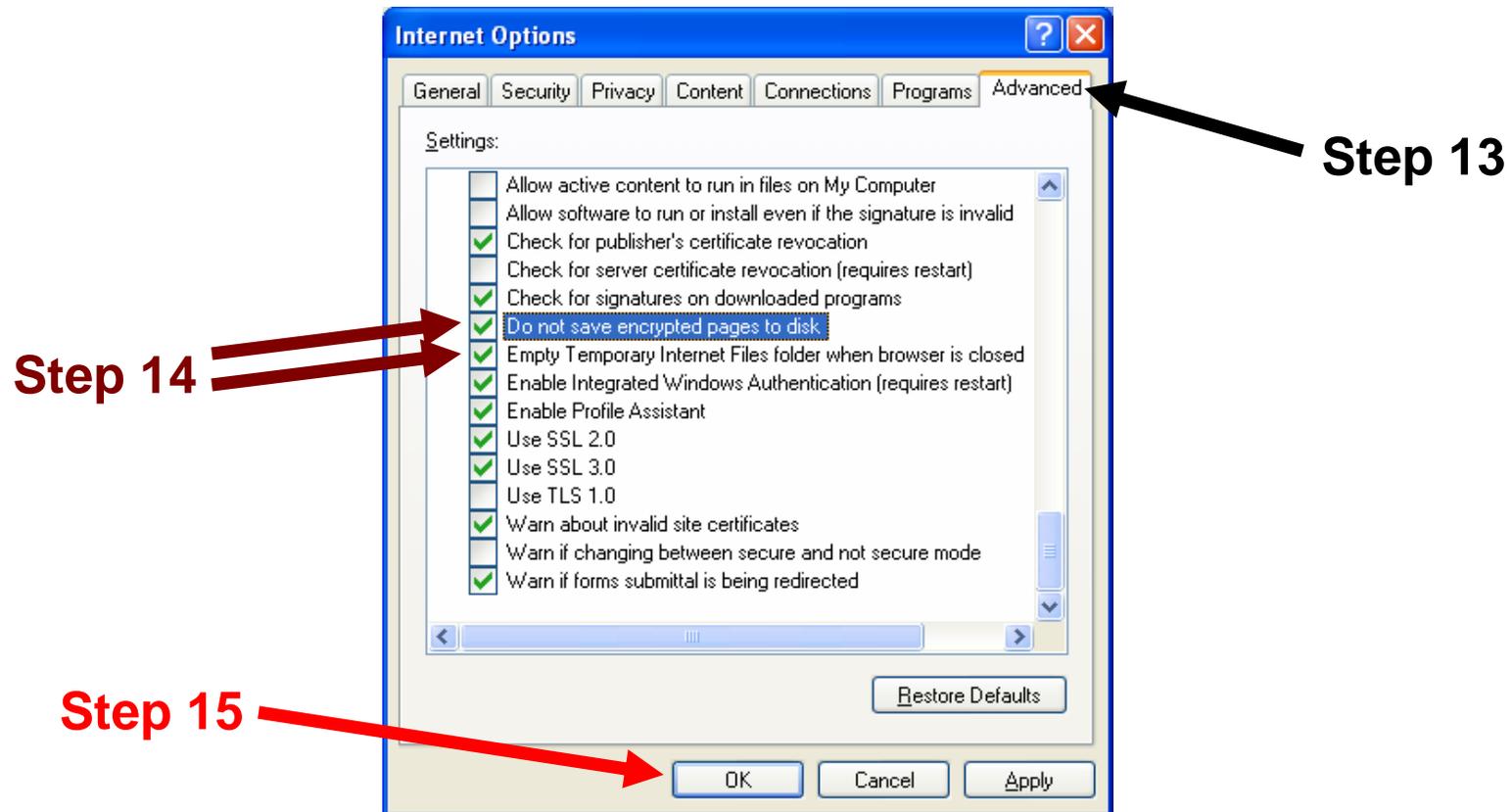
Fundamental Microsoft Internet Explorer Configuration



Step 11: Click on the **Content** tab and then click on the **AutoComplete** button

Step 12: Uncheck the **User names and passwords on forms** box and then click on the **Clear Passwords** button

Fundamental Microsoft Internet Explorer Configuration



Step 13: Click on the **Advanced** tab

Step 14: Scroll down, click on the **Do Not Save Encrypted Pages & Empty Temporary Internet...** boxes (so they are both checked)

Step 15: Click the **OK** button to accept all changes