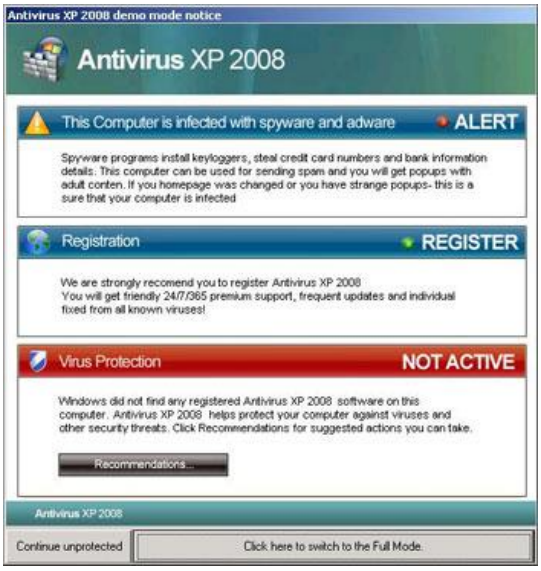
NORTHSTAR TECHNOLOGY SOLUTIONS

Internet & E-mail Best Practices

- ***Internet Browsing:***

  - **Security**
    - It is common practice to search the web to find desired content. Be aware that clicking on a link in search engines such as Yahoo, Google or Bing may redirect you to an infected website. Also, you can get viruses through legitimate websites.
    - Be mindful not to click "OK" on any pop-up error messages. Many viruses are executed by clicking "OK" or acknowledging the pop-up.
    - If you notice any suspicious behavior on your PC after using the web, contact your System Administrator immediately.

    - The following screenshots are examples of FAKE alerts:

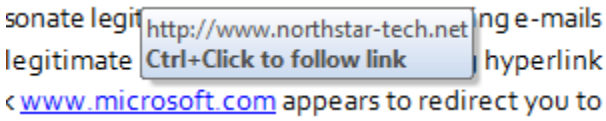


  - **Performance**
    - Do not watch video or listen to the radio over the internet during business hours. These types of connections use streaming files that take away from bandwidth required by mission critical applications and degrade internet performance to the entire company.
    - Terminal Server Users Only: Browse the internet through your local desktop. The Remote Desktop Protocol (RDP) cannot handle the video rendering requirements of current websites.

- ***Using E-mail:***

  - Do not open attachments or click on links in suspicious e-mails, many harmful e-mails contain phrases in broken English. A rule of thumb, if the offer seems too good to be true, it usually isn't.

  - Be aware of Phishing e-mails. Phishing e-mails impersonate legitimate sources. Many phishing e-mails contain links that appear to be directing the user to a legitimate website but the underlying hyperlink redirects to a different website. Ex., the following link www.microsoft.com appears to redirect you to Microsoft's website. If you hover your mouse over the link, a dialogue box displays the actually link, in this case www.northstar-tech.net.



  - Spam e-mail is usually not the result of an Employees actions but someone who has the Employees e-mail address in their address book. The e-mail address may be obtained by viruses that have infected a PC (frequently a home PC that does not updated security patches or virus definitions) and sends the PC's contact list to spamming servers. Once your e-mail address has been obtained by these servers, it is impossible to remove it. Most companies have a Spam filter service that filters inbound e-mail prior to delivering the message to the Mail Server or Inbox. If you notice an influx of spam messages, please contact your System Administrator.

- ***Recommended End User PC Best Practices:***

  - Log out of your network and turn your computer off overnight.

  - Keep your PC's security patches (Windows Updates) up to date. If you receive a message that new updates are available, contact your System Administrator. These updates can be set to automatically download and install without end user input.

  - Verify your Anti-Virus definitions are up-to-date. Due to the many different Anti-virus software vendors and configurations, check with your System Administrator for your company specific instructions. **Note:** This does not apply to users with Thin Client devices.