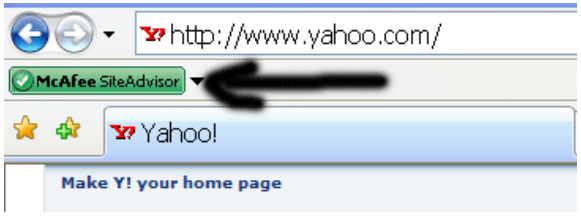
SITE ADVISOR Q-CARD

What is Site Advisor?

●SiteAdvisor Enterprise is a security add-on for Microsoft Internet Explorer and Mozilla Firefox browser that ***identify sites linked to spyware, adware, spam, viruses, browser-based attacks, phishing, or online fraud***.



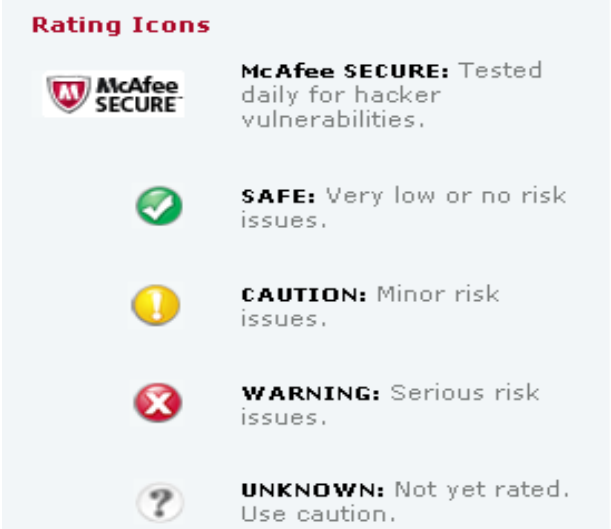
Using Search Engines

●The results from a search with Google, Yahoo or another search engine will show Site Advisor rating ***icons next to the website links***.

●By hovering your cursor over the icon, Site Advisor will provide statistics for downloads, sites linked to website, and pop-ups. This alerting feature helps you to avoid visiting malicious websites and downloading viruses and other malware onto your PC.

●Instead of clicking the links from the search results, which could possibly download malware to your computer, you can click on the **Site Advisor** icon to get additional information about the site.

Site Advisor Rating Icons Explained



What is Phishing

●Phishing is the practice of ***creating a website that replicates an existing legitimate website*** and is used to trick users into submitting personal, financial, or password data. For example, you may receive an email message containing a link to a phishing website that looks like a well known bank. Upon accessing that website, you are requested to enter your ID and password to verify the account. Unfortunately, the information you enter is collected to be used by hackers to access your bank account.

How to Avoid Phishing

●***Do not provide personal or financial information via email*** and do not respond to email solicitations for additional information. Do not click on links sent to you in email messages.

●Pay attention to the URL of a website site and look for inconsistencies. ***Malicious web sites*** may look identical to the legitimate sites, but the URL may use a variation in spelling or a different domain.

●If you are unsure whether an email request is legitimate, try ***to verify it by contacting the company directly***. Do not use the contact information provided in the email message. Instead, check previous documents you have that you know are from the legitimate institution.

●To take your phishing IQ test, go to http://www.sonicwall.com/phishing

Common Phishing Emails

●Communication from online payment services or other online providers (such as PayPal) claiming that there is a ***"problem" with your account and requesting that you access*** their web site to provide personal and account information.

●An email message pretending to be from the FDIC saying that the FDIC **is *refusing to ensure your account because of "suspected violations of the USA Patriot Act***." It requests that you provide information through an online form to "verify your identity".

●Communication purporting to be from ***an IT Department that asks for your password and other information*** that a phisher can use to penetrate the organization's network and computers.

●A low-tech version of the above will ask you to ***fax back information on a printed form that you can download from their phishing website.***

Additional Links to "How To" documents

●Additional training manuals located on website.
http://www.nocccd.edu/Departments/IS/InfoServicesTraining.htm#BannerTrainingManuals

●CaTT Tales Archives:
http://www.nocccd.edu/CaTTTales.htm

Contact Information

● IS Help Desk: 714-808-4849

● Email: ishelpdesk@nocccd.edu

Notes