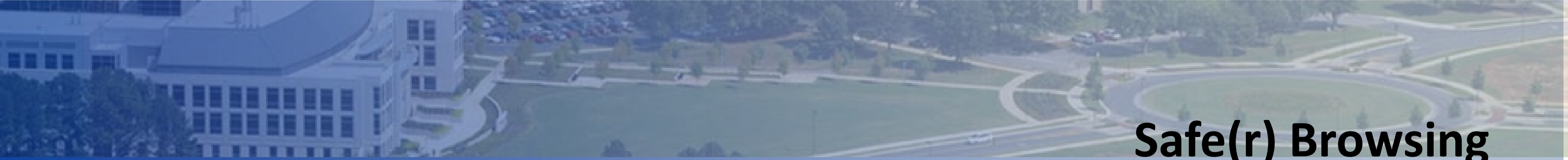
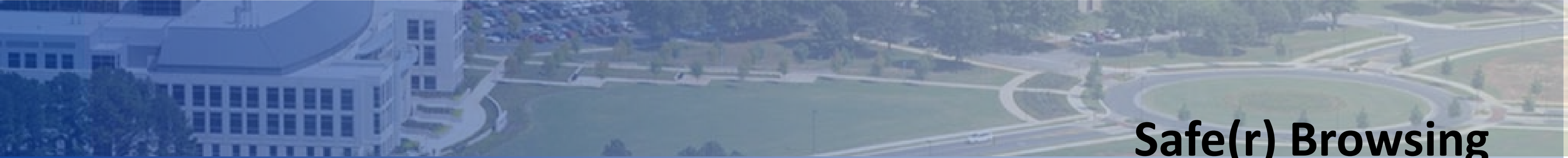


Safe(r) Browsing

Methods to Avoid Malware

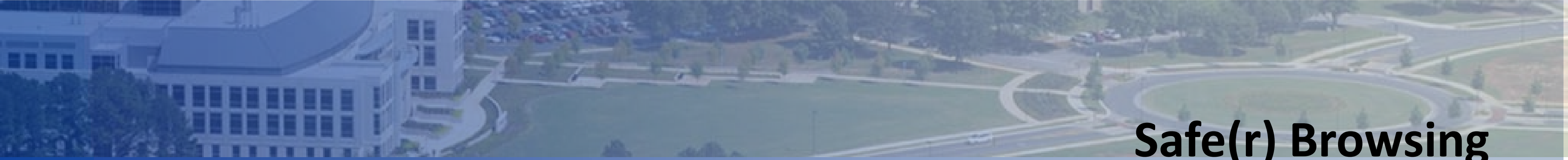


Why is important for me to know about malware?

- In the past, a user had to take some specific action, like opening an email attachment, for their computer to become infected with malware
- “Drive-by downloads” – Now simply visiting a website can cause your computer to become infected

Not Just on Naughty Sites Anymore

- Symantec claims *every one* of the top 100 websites in the world have served up malicious code at some point
- Top sites get malware from:
  - Infected Advertisements from third parties – lack of inspection
  - Hacked web-servers where hackers introduce code to the legitimate website



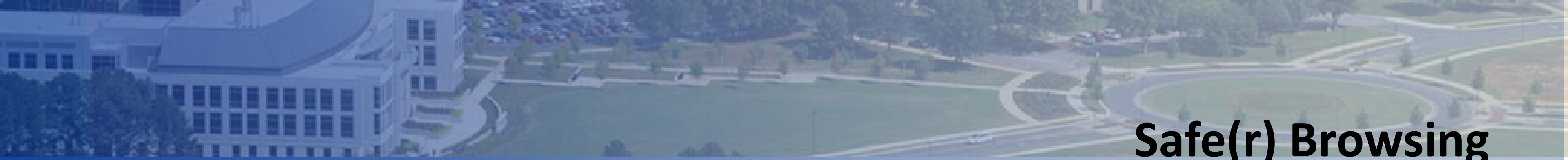
Safe(r) Browsing

The Basics

- Keep your browser up to date – don’t forget plug-ins (Flash, Silverlight, etc.)
- Make sure your Antivirus is running and up-to-date
- Run a host-based firewall

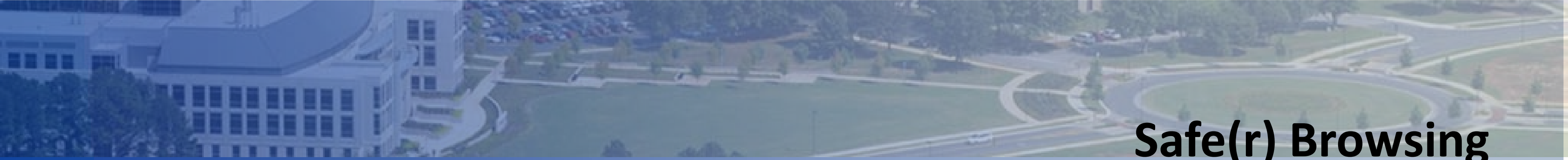
The Not Quite Basics

- Increase security settings for your browser of choice
  - Default Settings are often inadequate
  - All major browsers (IE, Mozilla Firefox, Safari, Google Chrome) have additional security settings that are not set by default
  - Check their websites for configuration information



The Not Quite Basics

- “Sandboxed” Browsers – runs the browser in an isolated space which prevents them from making permanent changes to other programs and data in your computer
  - Google Chrome – runs in a sandbox
  - Sandboxie – works with other browsers



Safe(r) Browsing

Things to watch for…

- Watch for URL (web address) that does not match the actual (look in lower left of browser while hovering over link)
  displayed: http://update.microsoft.com/microsoftupdate
  actual: http://64.208.28.197/ldr.exe
- Beware of link that executes a program (like *ldr.exe* above)
- Avoid numeric IP addresses in the URL
  http://168.234.153.90/include/index.html
- Some even use hexadecimal notation for the IP:
  http://0xca.0x27.0x30.0xdd/www.irs.gov/
- Watch for legitimate domain names embedded in an illegitimate one
  http://**leogarciamusic.com**/servicing.**capitalone.com**/c1/login.aspx

Safe(r) Browsing

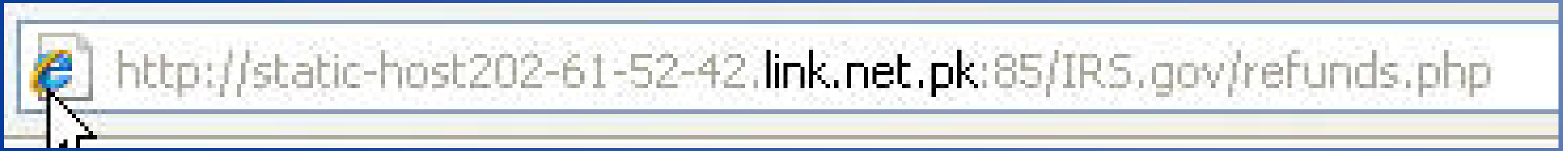
Things to watch for…

- Beware of email supposedly from US companies with URLs that point to a non-US domain (Kyrgyzstan in example below)

  From: Capital One bank <cservice@capitalone.com>

  URL in msg body: http://towernet.capitalonebank.com.**mj.org.kg**/onlineform/

- IE8 highlights the actual domain name to help you identify the true source. Here's one from an IRS scam email that's actually hosted in Pakistan:

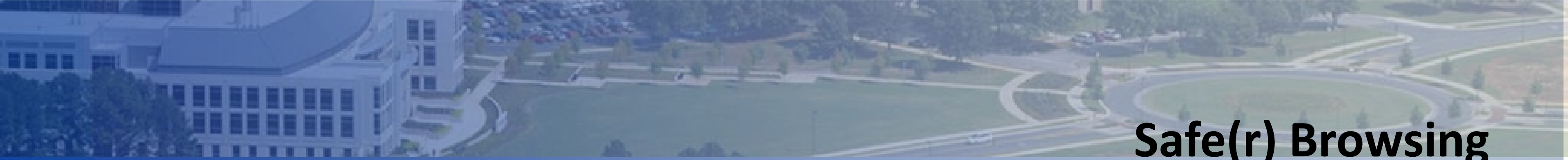


http://static-host202-61-52-42.**link.net.pk**:85/IRS.gov/refunds.php

Safe(r) Browsing

Things to watch for…

- Beware of domains from unexpected foreign countries
  Kyrgyzstan: http://towernet.capitalonebank.com.**mj.org.kg**/onlineform/
  Pakistan: http://static-host202-61-52-42.**link.net.pk**/IRS.gov/refunds.php
  Lithuania: http://**kateka.lt**/~galaxy/card.exe
  Hungary: http://**mail.grosz.hu**/walmart/survey/
  Romania: http://www.**hostinglinux.ro**/
  Russia: http://mpo3do.**chat.ru**/thanks.html
- Country code definitions available at:
  www.iana.org/domains/root/db/index.html



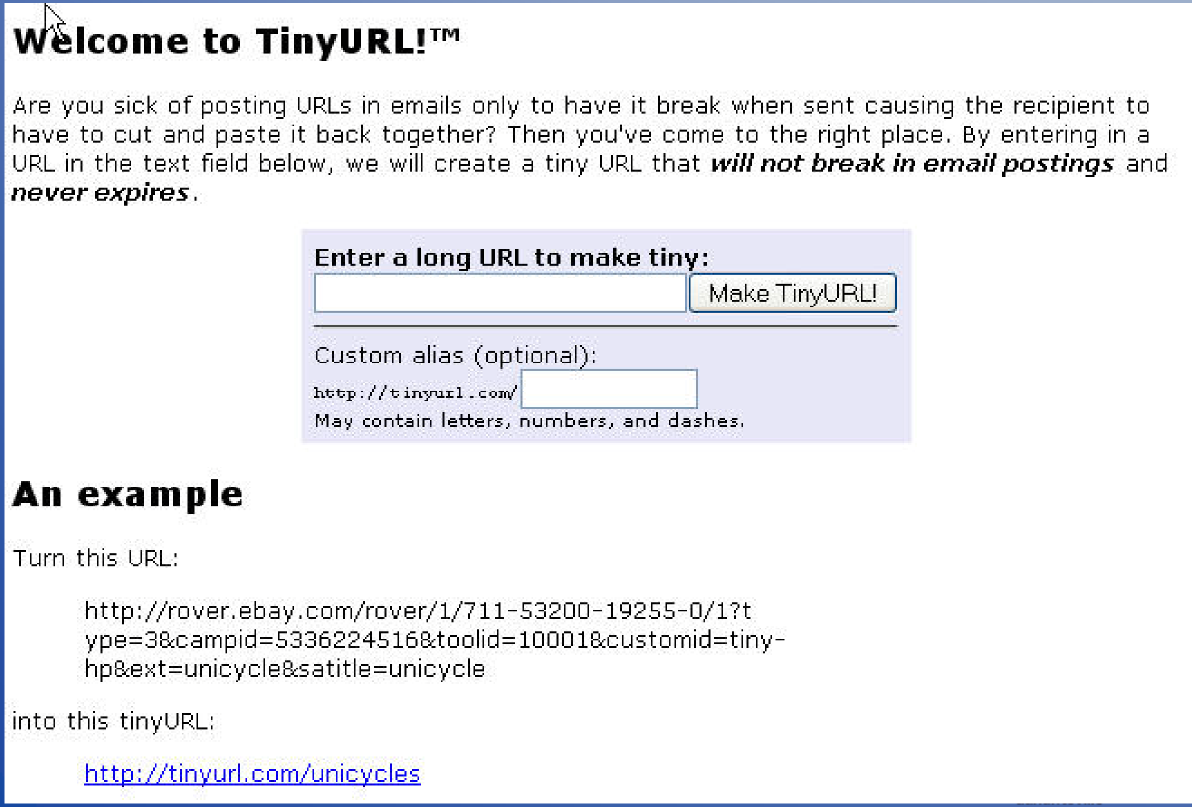
Safe(r) Browsing

What to do if you’re not sure…

- Analyze web links w/o clicking on them by copying the URL and testing them at this sites:
  - McAfee SiteAdvisor (enter URL on this web page – you don’t have to install their software): www.siteadvisor.com/
  - See “View a Site Report” on the right
  - ITS is considering adding SiteAdvisor through EPO

Be Careful with Shortened URLs

- Watch for malicious URLs cloaked by URL shortening services like:
  - TinyURL.com
  - Bit.ly
  - CloakedLink.com



Welcome to TinyURL!™

Are you sick of posting URLs in emails only to have it break when sent causing the recipient to have to cut and paste it back together? Then you've come to the right place. By entering in a URL in the text field below, we will create a tiny URL that ***will not break in email postings*** and ***never expires***.

Enter a long URL to make tiny:
Make TinyURL!
Custom alias (optional):
http://tinyurl.com/
May contain letters, numbers, and dashes.

An example

Turn this URL:

http://rover.ebay.com/rover/1/711-53200-19255-0/1?type=3&campid=5336224516&toolid=10001&customid=tiny-hp&ext=unicycle&satitle=unicycle

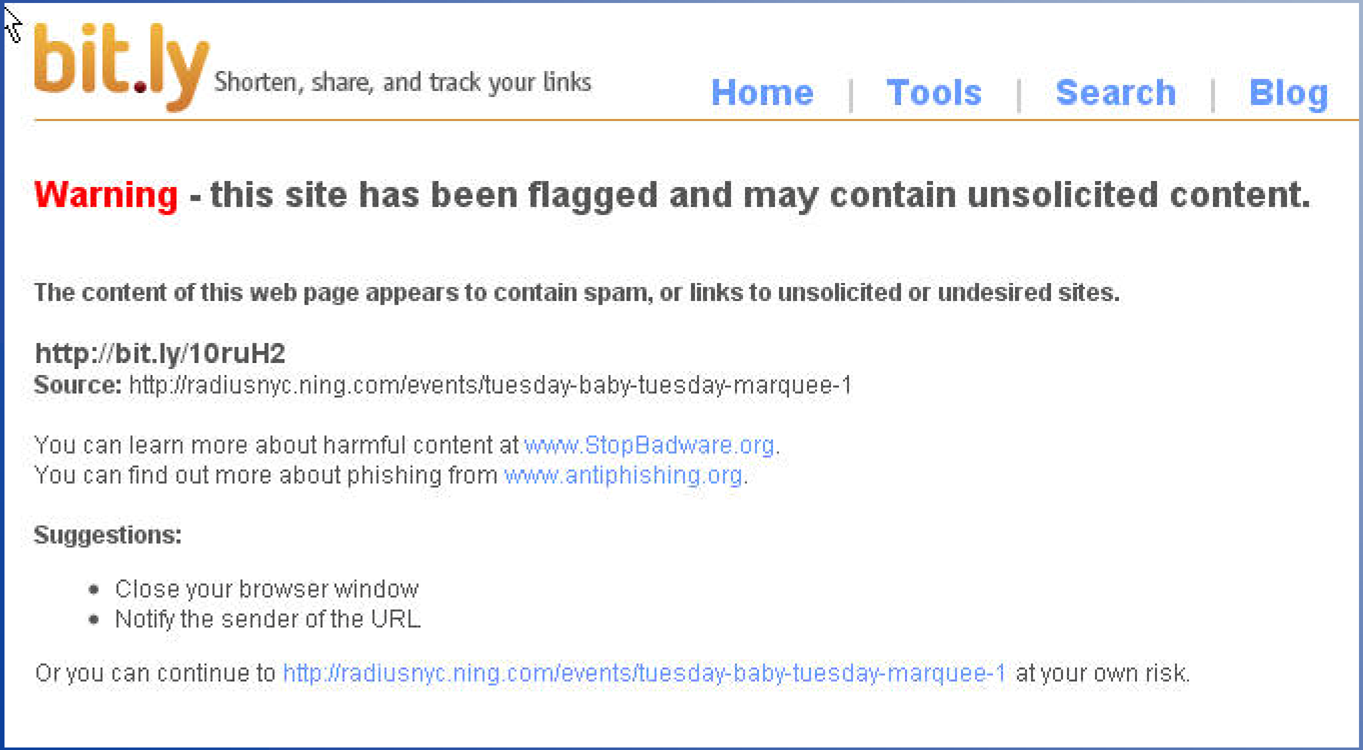
into this tinyURL:

http://tinyurl.com/unicycles

Be Careful with Shortened URLs (Cont.)

- TinyURL has a nice “preview” feature that allows you to see the real URL before going to the site. See tinyurl.com/preview.php to enable it in your browser (it sets a cookie)
- Bit.ly has a Firefox add-on to preview shortened links:
  addons.mozilla.org/en-US/firefox/addon/10297
  It also warns you if the site appears to be malicious:

Be Careful with Shortened URLs (Cont.)


bit.ly
Shorten, share, and track your links
Home | Tools | Search | Blog

Warning - this site has been flagged and may contain unsolicited content.

The content of this web page appears to contain spam, or links to unsolicited or undesired sites.

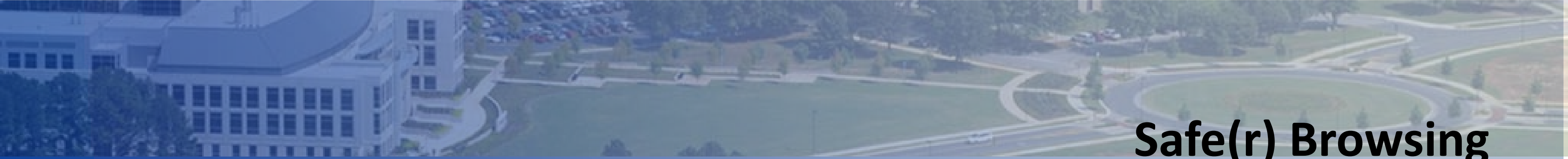
http://bit.ly/10ruH2
Source: http://radiusnyc.ning.com/events/tuesday-baby-tuesday-marquee-1

You can learn more about harmful content at www.StopBadware.org.
You can find out more about phishing from www.antiphishing.org.

Suggestions:

- Close your browser window
- Notify the sender of the URL

Or you can continue to http://radiusnyc.ning.com/events/tuesday-baby-tuesday-marquee-1 at your own risk.



Questions?