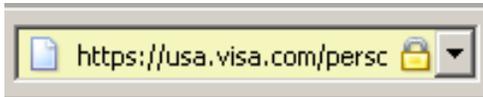


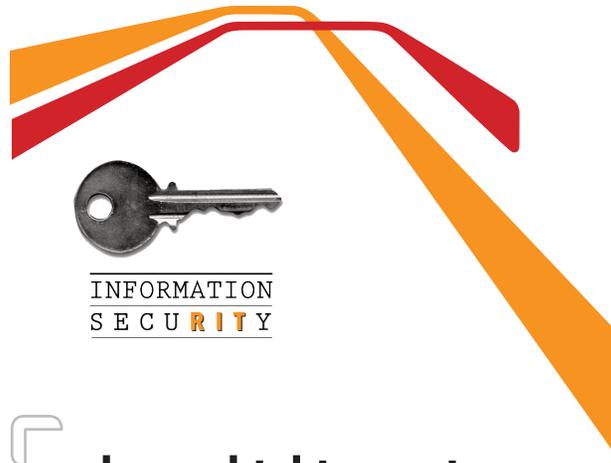
safe practices

- It's not always safe to just click on a link! Enter or copy the link into the address bar or go to the institution's website and navigate to the correct location as you normally would.
- Check the properties of websites before entering information. You can check the properties from the file menu or by right-clicking on the web page and selecting properties.
- Secure web sites use a technique called SSL (Secure Socket Layer) that ensures the connection between you and the website is private. The use of SSL is indicated by "https://" (instead of "http://") at the beginning of the address AND by a padlock icon, which must be found either at the right end of the address bar or in the bottom right-hand corner of your browser window. (A padlock appearing anywhere else on the page does not represent a secure site.)



anti-phishing tools

There are a number of tools available to help warn you of suspicious websites. Use one or more for your protection. For an updated list of anti-phishing tools, visit the RIT Information Security Phishing page at <http://rit.edu/security/content/phishing>.



take a phishing quiz

Do you think you can identify a phishing attempt successfully? Find out by taking the SonicWall phishing quiz at <http://www.sonicwall.com/furl/phishing/>.

get informed

Visit the RIT Information Security website to read the security standards, get the schedule for our Digital Self Defense workshops, access security tools and software, or find out more ways to protect yourself.

RIT INFORMATION SECURITY

<http://rit.edu/security>

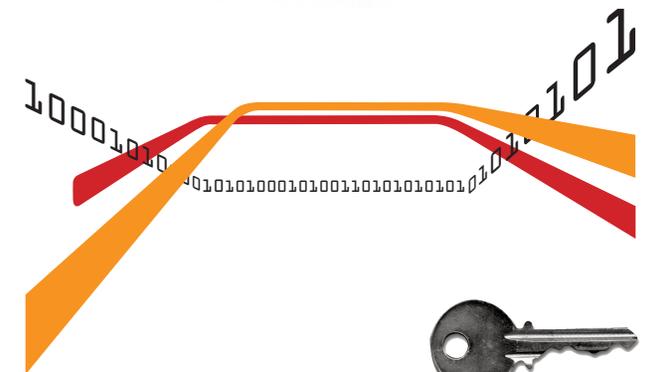
infosec@rit.edu

(585) 475-4123



DIGITAL SELF DEFENSE: avoiding identity theft online

Detecting Online Scams & Phishing



Revised 7/17/2013

