Safe Browsing and Sensitive Data

Stay safe online and learn about restricted data

Andrea Childress
Director, Systems and Programming

Safe Browsing

- Log out of and close browser windows when you're finished with a site especially on public machines
- If conducting financial business make sure the site is reputable and secure via https:// and the padlock icon. Be cautious, no indicator is foolproof; some fraudulent sites have forged security icons. It's best to know who you're dealing with.
- Don't store sensitive information on your machines or devices (SSNs or Tax forms i.e. W2, etc)
- Don't allow web sites you use to save your credentials
- Password protect all of your devices (desktop, laptop, tablet, phone, etc)
  - 45% of data breaches at companies are caused by lost laptops and mobile devices (2012 study by the Ponemon Institute)

Social Security and Credit Card Numbers

- You are not authorized to store Social Security or Credit Card Numbers in any way (hard drive, shared drive, flash drive, jump drive, email, spreadsheet, Word doc, web page) unless you have acquired an exemption from the CIO.
- Use Spider to identify and eliminate SSNs and CCs in your control
- If you don't need it, delete it
- If you need it but can replace it with NUID contact ITS
- If you have to use it for your job, talk to the CIO