Sensitive Data Scanner

# Instructions:  Spider for Windows

## Short Version

Below are simple instructions (intended for more advanced users).  By clicking on any of the numbered links you'll be directed to a more detailed explanation of each step.  The instructions are written specifically for Windows Vista, but the overall process is the same for any Windows operating system.

1. System Requirements

   Spider for Windows has the following minimum system requirements:

   - Windows version 2000 or later (2000, XP, Vista, 7)
   - .NET Framework Version 2.0 (or newer)

   Make sure your workstation meets the minimum requirements before proceeding.

   It's not required, but in order for Spider to perform a full system scan, the user needs to have Administrative privileges on the target machine.  If you do not have Administrative privileges, speak with your IT support staff on how to proceed.

2. Download and install Spider

   Spider can be downloaded from the following url:

   http://www2.cit.cornell.edu/security/tools/Spider_Release_2008.zip

   The default installation settings should work for most users.

3. Delete Temporary Internet Files

   "Temporary Internet Files" are local files stored by your web browser to enhance the web browsing experience.  Deleting these files will both increase Spider's scan speed and reduce the number of false positives reported.  As a general best practice these files should be cleaned regularly.

4. Empty the Recycle Bin

   Similar to the Temporary Internet Files, the computer's Recycle Bin should be emptied to minimize the number of files Spider will scan.

5. Launch Spider

   Run spider4.exe and start the program.

6. Configure Spider

   Configuration changes that should be made:

   - Change the root scan path to "C:\" or the drive label of your primary hard drive.
   - If you have multiple hard drives, set Spider to search each one.

7. Run Spider

   Scan your system for SSNs and CCNs.

8. Verify and Fix Findings

   Manually inspect each file flagged by Spider.  Ignore false positives, and secure or delete Restricted Information.  Typically files containing Restricted Data are more likely to appear in your "My Documents" or other folders where you typically store your files. They are less likely, but certainly plausible to appear in folders such as "Program Files" or "Windows".

   A simple outline of this process follow:

   1. Inspect the file.
   2. Determine if the file contains Restricted Information.
   3. Delete, secure, or relocate sensitive files.

   Some things to consider when you find Restricted Data:

   - Do I still need this information?

- Are there record retention laws pertaining to this information?
- Where did I get this information?
- Do any of my coworkers have this information?
- Is my copy the sole source of this information?
- Have I ever sent this information to anyone?
- Will I be receiving more data like this?
- Is this data stored anywhere else that I know of?

9. Cleanup

   The output generated by Spider inherently contains sensitive information. After running a scan, it's necessary to remove the scan logs and databases. The cleanup consists of two steps:

   - Remove Spider scan database
     - The Spider scan database is located in C:\Users\USERNAME\AppData\Local\Spider\State where USERNAME is your Windows username.
   - Uninstall Spider

10. Complete Survey

    Your feedback is vital to the success of this project. In order to ensure the effectiveness of this document, we'd like to hear any and all opinions about its structure, content, flow, grammar, or any other issues or observations you might have noticed.

    Please visit this webpage and complete the survey. You'll need to log in using your UCSB NetID.

    Thanks again for your participation.