Preventing ID Theft with Identity Finder for Windows

Introduction

Identity Finder is a tool used to scan your computer, file shares or external media for Personally Identifiable Information (PII) such as Social Security Numbers, credit card numbers, bank account numbers and passwords. The Identity Finder Software will assist you with easily deleting or protecting the resulting data. Many people who run Identity Finder for the first time are shocked by how much of their own PII is hidden on their computers just from daily use.

Sources of PII @ Carnegie Mellon

_____

_____

_____

_____

_____

_____

Identity Finder Resources

Computing Services Documentation & Installer Download
https://www.cmu.edu/computing/doc/security/identity/index.html

In Program Help
Start Menu -> All Programs -> Identity Finder -> Identity Finder Help

What To Do If You Suspect A Breach

Procedure for Responding to a Compromised Computer
https://www.cmu.edu/iso/governance/procedures/index.html

Identity Theft Resources

FTC: Deter. Detect Defend. Avoid ID Theft
http://www.ftc.gov/bcp/edu/microsites/idtheft/

Proper PII Handling

1. Secure Your Computer

   Computing Services: Secure Computing & Step by Step Guides
   https://www.cmu.edu/computing/security/index.html

2. Know What You Have
   - Find out what PII is stored on your computers, servers and media using Identity Finder.

3. Delete or Secure Regularly
   - Clean up PII regularly to keep it from piling up.
   - You decide how often depending on how much PII you handle.
   - Run Identity Finder before trips.

4. Transfer Securely
   - Use encrypted communication methods or only send encrypted files.

   Identity Finder's Secure Zip

   PGP Desktop
   http://www.pgp.com/products/desktop_home/index.html

   TrueCrypt (Open source – Windows, Mac, Unix)
   http://www.truecrypt.org/

5. Physically Store Securely
   - Be mindful of potential theft; lock up your equipment and media including backups

6. Proper Disposal
   - Cleanse storage devices BEFORE disposing, decommissioning or giving away.

   Guidelines for Data Sanitization & Disposal
   https://www.cmu.edu/iso/governance/guidelines/data-sanitization.html

   Data Sanitization and Disposal Tools Matrix
   https://www.cmu.edu/computing/security/secure/tools/data-sanitization-tools.html

7. Evaluate Workflow
   - Eliminate usage of PII where possible.
   - Challenge the status quo.

8. Remain Vigilant
   - Trust but verify.
   - Stay aware.

   Computing Services: Getting News
   https://www.cmu.edu/computing/news/getnews/index.html