Learn About Spirion (formerly Identity Finder)

Stephanie Obodda - 2019-09-13 - 0 Comments - in Spirion Identity Finder

To find and secure confidential information on your computer, the Information Security Group recommends that you install and periodically run Spirion (formerly known as Identity Finder), which lets you hunt down PII (personally identifiable information) such as passwords, social security and credit card number, and then to secure it. Brown's enterprise version is available to all active faculty and staff.

Here are the basic steps to using Spirion, followed by an FAQ.

1. **Install** Spirion. Faculty/staff can find it in the Software Catalog at [Spirion (formerly Identity Finder)](1).
2. **Activate** the software. Create a password to secure your reports.
3. **Define your search**: what drive(s), types of files, kinds of PII. ISG recommends configuring your search for your own hard drive and to detect credit card and social security numbers (highest risk and fewest false positives).
4. **Protect any PII** found by destroying or securing it (options include Shred, Scrub, Secure and Quarantine).
5. **Schedule regular runs.** How often depends on what kinds of PII you routinely deal with (once a week if so, quarterly at a minimum).
6. **Questions** about using the software? Check out the [Windows](2) and [Mac](3) online manuals.

---

- **What is Spirion?**
- **What is the objective of making Spirion available here at Brown?**
- **Who can use it?**
- **What operating systems does Spirion run on?**
- **Where can I find it and how do I install it?**
- **Do I need to have Spirion password (requested upon install)?**
- **What type of files does Spirion search and where?**
- **What should I be searching for?**
- **How do I use Spirion to search for sensitive data?**
- **Once sensitive information is discovered, what actions can be taken?**
- **Is my personal information being collected somewhere?**
- **Is it possible for anyone to see details of my PII?**
- **Can anyone suffer negative consequences as a result of running Spirion?**
- **How often should I run Spirion?**
- **What if Spirion identifies something as a Social Security or credit card number, but it's not and I want to keep the info as it is. Will this come up every time I do a scan?**
- **What if I need help with Spirion?**

**Q. What is Spirion?**

**A.** Spirion is software that helps prevent identity theft and aids in keeping Brown compliant with federal and state laws by detecting and securing sensitive data on your computer. Spirion is able to detect patterns -- such as those for Social Security, credit card and bank account numbers, references to passwords and other customizable data that you would specify.

**Q. What is the objective of making Spirion available here at Brown?**

**A.** Adding regular scans with Spirion to other information security measures already in place helps Brown to not only remain in compliance with regulatory and legal obligations, but also to lower its (and the individual user's) level of risk.

**Q. Who can use it?**

**A.** All active employees -- faculty and staff -- can download and install the full enterprise version of Spirion from the Software download pages (see links below) onto their Brown computers.

**Q. What operating systems does Spirion run on?**

**A.** Spirion is available for the following versions of Windows and Macs:

- Supported Windows versions: Windows 7, 10
- Supported Mac versions: OS 10.9 or later

**Q. Where can I find it and how do I install it?**

**A.** You can download both Windows and Mac versions from the [Software Catalog](#).
Q. Do I need to have a Spirion password (requested upon install)?
A. You do not need to use a password, signing on as a guest instead. However, a password is necessary to protect any search you wish to save and the sensitive information contained within that file. For this reason, it is recommended that you do use a password, but with care, since if you forget your password, you will be unable to load your saved results nor login to the application.

Q. What type of files does Spirion search and where?
A. Spirion searches can be configured to search your entire hard drive (whether on a laptop or desktop), as well as external drives for many file types including:

- Microsoft Office files
- PDF files
- Compressed files
- Cached websites and cookies
- Registry keys

Q. What should I be searching for?
A. To meet regulatory compliance, ISG recommends searches that target social security and credit card numbers. This data is at highest risk and searches for it produce the fewest false positives. After an initial search and you secure any data found, you can broaden your search to other sensitive information (i.e., anything that if lost could present a risk to Brown, you, or someone else). See the Data Risk Classifications document for a listing of data by level of risk.

Q. How do I use Spirion to search for sensitive data?
A. The user guides (Windows | Mac) provide a good overview as well as step-by-step instructions for using Spirion. Note that upon install, the final screen asks if you want to run a scan. You can do so then or wait until a later time.

Q. Once sensitive information is discovered, what actions can be taken?
A. You should take appropriate action and then rerun Spirion to ensure all sensitive information is either removed or protected. After a scan, you will be presented with a report of its findings, which will list any sensitive information found that matches your search
criteria and its location. You can save the file for later action on it (requires a password) or take immediate action. Your choices include:

- **Shred:** Use this option if you wish to permanently remove any files that contain sensitive information. Use Shred ONLY when you no longer need that information as shredding is not reversible, and once removed, it cannot be retrieved.
  
  *Example:* An old Excel spreadsheet listing student workers and their social security numbers.

- **Scrub:** Use this option when you locate a match on sensitive data and wish to remove just that data but leave the rest of the file intact. Note that scrubbing (also referred to as redacting) is limited to certain file types.
  
  *Example:* An Excel spreadsheet listing current workers, their emergency contact information, birth dates and social security numbers. Since the information is still relevant, remove the social security numbers, and if you don't need them, the birth dates as well.

- **Secure:** Use this option when sensitive information is identified but you wish to keep it and the context in which it is located. The Secure option lets you encrypt and password-protect the file to prevent unauthorized individuals from accessing it. Note that this option is handy when you discover sensitive data files but don't have the time to immediately remove them.
  
  *Example:* As in the above example for Scrub, but as the department financial manager you need the employees' social security numbers at this time.

- **Quarantine:** Use this option when a file has sensitive identity match information in it and you wish to securely move the file to another location. Quarantine will move your file and then shred the original so that it cannot be recovered by anyone who gains access to your computer. It is important that you quarantine files to a location that is highly secure, such as an encrypted drive or a storage device to which unauthorized individuals do not have access.
  
  *Example:* An Excel spreadsheet with sensitive information of former employees. There is no current need for it but for legal and historical reasons you wish to preserve the file.

**Q. Is my personal information being collected somewhere?**

**A.** The Information Security Group (ISG) is collecting summary data such as the number of passwords, social security numbers, credit card and bank account numbers found during a Spirion scan. This data is analyzed to track what is being found and if the risk is then being addressed, which keeps Brown in compliance with identity theft legislation.

**Q. Is it possible for anyone to see details of my PII?**
While this level of granularity is available, the ability to view this detailed PII is limited to high level information security staff, who do not view this information as there is no need. As with other personnel at Brown who have access to student, HR and financial information, ISG staff are bound by a confidentiality agreement to respect the privacy of others.

Q. Can anyone suffer negative consequences as a result of running Spirion?
A. No, there are only benefits to doing so. It will let you know whether or not you have PII that needs to be protected and gives you the means to remove or protect it. It will also raise your awareness about introducing any new PII onto your computer so that you can take appropriate action at the time. Regular scans will reduce your individual risk as well as Brown’s institutional risk. Should PII be detected, no data will be deleted by the Spirion administrators, nor will individual data be accessed without business need (following the Emergency Access Policy), or equipment removed because of the data that is found.

Q. How often should I run Spirion?
A. It depends on the level of possible risk. If you’re dealing with sensitive data on a regular basis, it is recommended that you run Spirion weekly, which can be configured to run automatically. Because it runs so quickly and in the background, we recommend that you run Spirion at least quarterly to ensure that your machine is free of restricted data. And in the event your computer is lost or stolen, this will not only provide peace of mind that you have not put any restricted information at risk but can report this to ISG.

Q. What if Spirion identifies something as a Social Security or credit card number, but it’s not and I want to keep the info as it is. Will this come up every time I do a scan?
A. This is an example of a false positive, which does occur occasionally. You can configure Spirion to ignore it on successive scans.

Q. What if I need help with Spirion?
A. For assistance with using Spirion, its Online Help is quite comprehensive and a good place to start. You may also want to consult their user guides: Windows | Mac. For questions about policy and/or procedures, contact ISG@brown.edu.

Tags
Security