Why is ITS putting Identity Finder on my University computer?

Tell Me

Info

University computers are required to have Identity Finder unless the department Information Security Liaison or Data Security Officer has documented a business need and risk mitigation plan for that exception.

1. ITS is responsible for securing the University’s resources and data as much as possible.
2. Individual users are also responsible for knowing and following the data handling guidelines.
3. Since it is technically possible to store unauthorized sensitive data on the hard drive (C:), which is not compliant with the data handling guidelines, ITS is responsible for minimizing that risk as much as possible.
   a. To help minimize that risk, ITS has purchased Identity Finder.
4. This tool supports efforts already underway to protect data and educate clients on appropriate storage of sensitive information.
5. Identity Finder is also used by some of our sister institutions such as UNC-Chapel Hill, NCSU, and Appalachian State.

Note

Information Security can’t see the information, the system only detects data that seems to meet social security and credit card number criteria.

Related FAQs

- What is Identity Finder and what does it do?
- What happens if Identity Finder finds SSNs or credit card numbers on a computer?
- Does Identity Finder scan University computers when they are off campus?
- Will the Identity Finder scan affect my computer’s performance?
- What types of data, or information, does Identity Finder look for?