University of Scranton
Information Security Office

Identity Finder Proposal – Automating Scans

Identity Finder is a software application that reduces the risk of data loss and identity theft by discovering and securing sensitive information across the University. This tool has been available for individual use by staff and faculty since 2009.

What is Identity Finder?

Identity Finder is a software application that helps prevent data loss and identity theft by locating files containing restricted information on your computer, network share drives, and external media. The Identity Finder application allows actions to be taken on files such as shredding the files, moving them to a quarantine location, or scrubbing the Personally Identifiable Information (PII) data from them.

What is Restricted Information?

Restricted information is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. Restricted information is generally regulated by law or contract and often used for financial, medical, or research identification. Examples of restricted data as noted in University policy include Social Security Numbers, credit or debit card numbers, bank account numbers, PIN numbers, driver's license numbers, and account passwords. Refer to the Information Classification Policy for additional information.

Why Clean Up this Data?

If your computer or external media contracts a computer virus, is lost, stolen, or broken into over the network, files containing restricted information are at risk for theft. A surprising amount of restricted information may be stored on your computer, external media, or network share drives from daily use. This information can be used to steal not only your money and identity, but also the money and identities of anyone else who either shares your computer or whose restricted information you store. If you store restricted information for University work, the University would be obligated under state law to notify everyone affected by the breach and could potentially be legally liable.

What Can We Do to Protect Restricted Information?

The Information Security Office in collaboration with the IT Client Services group is proposing that we automate scanning for restricted information in order to ensure that it is happening on a regular basis on University-owned desktops and laptops. This would mean that scans would be scheduled by the Information Security Office to run on a regular basis using the Identity Finder application to search University machines for restricted information.

What Happens When We Find Data?

The Information Security Office will alert and work with individuals and their division or college's data steward to ensure that the information is properly secured or disposed of if no longer needed. The Information Security Office will identify ways to minimize the exposure of the information without impacting the work of the individual or department involved.

What We Will Not Do

We are only looking for University information that is classified as restricted. The Identity Finder application does not allow us to see what individuals are doing or read your files. The software application will only provide us with the string of numbers or characters that match the potential restricted data and the location of the information. If restricted information is found, it will not be shared with anyone outside of the Information Security Office and the division or college data steward.

What are the benefits?

Automating the scans conducted using Identity Finder will reduce risk of information loss or identity theft for the University by identifying and minimizing the number of locations that restricted data is stored.

This application will also help shorten the time it takes to process and return a machine to individuals if the device is infected because the regulated, restricted data will already have been identified and secured.

March 2013