



Protect Your Business Identity

By Eric Haas
February 5, 2009

Having your identity stolen can completely change your life and take years to overcome. Now imagine a business getting its identity stolen. How does a business begin to recover from a ruined credit history and possibly large amounts of debt? A stolen business identity could be the beginning of a financial disaster that could last for years.

Business identity theft is more common than most people think and becoming part of a business identity theft statistic can happen to anyone. No matter what type of business you have, if the wrong person is at the right place, they could have access to documents or materials you thought you destroyed properly.

There are a few simple precautionary steps to take to protect your business from identity theft:

- Protect computers – Many employees have access to business computers. Employee access to programs or databases containing sensitive information should be reviewed regularly. Password protect as many files as possible and always use passwords and install firewalls to protect your network. When making purchases online on your business computer, set security options to a higher setting on your computer since the default will allow just about anything to be downloaded.
- Shred documents – Any type of business records should never be tossed in the trash or recycled. Keep in mind that discs and other media containing sensitive information should also be shredded. Consider utilizing businesses that are available to shred documents for you. For additional reassurance, utilize a company that is NAID AAA (National Association of Information Destruction) certified. This certification signifies excellence in secure information destruction services.
- Use locks, keys and alarms – Businesses should have alarm systems to deter break-ins. Be sure windows are secured with screens or shatter-proof glass. Whenever you are not using the information, you should always keep customer records and other data on paper in locked filing cabinets. Important business data such as database backups should always be stored in a safe, secure area.

Don't forget to review and update your company's security policies and be sure all employees are up to date on those policies. Discuss your e-mail and Internet policies, computer network access, how to increase browser security settings and how to deal with suspicious mail or e-mails. Be sure your employees know to contact you if they notice any suspicious activity. Keep in mind that when an employee no longer works for your business, you need to make sure their access to company data or your computer network is immediately cut off.

There are a lot of great resources and new technologies available for business owners that can play a role in protecting the business' identity. The best part about taking these precautionary steps is that they are neither time consuming nor costly to implement and they could potentially save you from a disaster that could take months or years to overcome.

Eric Haas is president of Automated Records Management Systems. Founded in 1983, Automated Records Management Systems provides information management and protection services to businesses throughout Wisconsin and Upper Michigan.

