Simple Safeguards:
Information Protection for Organizations

Physical Security

- Take stock of what personal information you have. Keep only what you need for your business.
- Records you need should be protected by layers of security. All layers, including outer building, inner office and record storage areas should be secure from unauthorized entry.
- Protect digital media with the same secure safeguards as physical records.
- Personal information inside a business should be protected during regular hours if the area is not monitored.

Computer Security

- Ensure your computer is protected with a firewall and against viruses and spyware. Update this software and operating systems on a regular basis.
- Make sure all wireless access is encrypted and accessible only through a user created strong password.
- Use strong passwords to protect computer access. Don’t store passwords on computer hard drive or post near the computer.
- Employees should memorize passwords and should be required to change them every 90 days.
- Set computers to log-off automatically after a few minutes of non-use.
- Restrict the use of laptops to employees who need them to do their job.
- Limit take home laptops. If they most go home, remove or encrypt personal information from them or any other digital media that leaves the office.
- Require employees to store laptops in a secure place. Never leave a laptop visible in a car.
- Limit download capability on employee's computers.
- Make sure a Web site has 128 bit encryption before conducting transactions.

Policy - Personnel - Training

- Establish and enforce a company-wide policy related to personal information.
- Regularly train employees to be sensitive to identity theft issues and personal information protection.
- Create a culture of security by holding employees accountable to the company policy.
- Have a defined and required way to report violations and suspicious activity related to information security.
- Establish a need-to-know policy and compartmentalize personal information to only those in your company who have a legitimate need to know before granting access.
- Disconnect ex-employees immediately from access to any personal information.

Information Security

- Use secure shredders or a secure shredding service.
- If you outsource shredding, make sure the shredding company complies with security standards such as employee background checks.
- Be cautious on the phone. Positively identify callers before providing personal information.
- Don’t e-mail personal information. This method is not secure.

Provided by
(Retired) FBI Special Agent Jeff Lanza
Web Site: www.thelanzagroup.com

Resources on the Web:

www.ftc.gov/privacy **www.ftc.gov/infosecurity**
www.sans.org **www.onguardonline.gov**