

Simple Safeguards: Identity Theft Prevention for Organizations

Presented by
FBI Special Agent Jeff Lanza
(Retired)

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.

Speaker Information: Jeff Lanza

Phone: 816-853-3929

Email: jefflanza@thelanzagroup.com

Web Site: www.thelanzagroup.com

Resources on the Web:

www.ftc.gov/privacy

www.sans.org

www.ftc.gov/infosecurity

www.onguardonline.gov

Simple Safeguards: Stopping Identity Theft Before it Stops You

Presented by
FBI Special Agent Jeff Lanza
(Retired)

1. Protect Your Personal Information

- ✓ Protect your social security number. Don't provide it unless required and never write it on checks.
- ✓ Photocopy the front and back of all the credit cards you carry in your wallet and store the copy in a safe place.
- ✓ Never routinely carry your social security card, passport, or birth certificate with you.

2. Protect Your Documents

- ✓ Shred your confidential trash with a cross-cut or diamond cut shredder.
- ✓ Don't leave outgoing mail with personal information in your mailbox for pick-up.
- ✓ Retrieve mail as soon as possible after delivery and avoid leaving it in your mailbox overnight.

3. Be Vigilant Against Tricks

- ✓ Never provide personal information to anyone in response to an unsolicited request.
- ✓ Never reply to unsolicited e-mails from unknown senders.

4. Protect Your Communications

- ✓ Ensure your computer is protected against viruses and spyware and set to update often.
- ✓ If you have wireless internet, make sure it is password protected.
- ✓ Make sure your cordless phone is digital and has a frequency of at least 900MHz.

5. Check Your Credit Report

- ✓ Order your credit reports at least three times per year (free).
- ✓ Check financial accounts often and investigate any unusual activity.

Credit Reporting Bureaus

Equifax: (800) 525-6285
P.O. Box 740241 Atlanta, GA 30374
Experian: (888) 397-3742
P.O. Box 9530 Allen, TX 75013
Trans Union: (800) 680-7289
P.O. Box 6790 Fullerton, CA 92834

Credit Reports

You are allowed 3 free reports each year; to order:
On Web: www.annualcreditreport.com
By Phone: 1-877-322-8228

To Report Internet Fraud:

www.ic3.gov

Key Numbers

FBI (202) 324-3000 or your local field office
FTC 1-877-IDTHEFT
Postal Inspection Service 1-877-876-2455
IRS 1-800-829-0433
Social Security Administration 1-800-269-0271

IF YOU ARE A VICTIM

1. Contact any one of the three credit reporting agencies and place a **fraud alert** on your account.
2. Contact affected financial institutions.
3. Contact affected creditors.

IF A LOVED ONE DIES

Send a copy of the death certificate to the three credit reporting agencies.

To remove your name from mail and phone lists:

- www.dmachoice.org
- www.donotcall.gov (1-888-382-1222)

To stop preapproved credit card offers:

- 1-888-5-OPTOUT (567-8688)

Credit Monitoring and Identity Theft Protection

Two options to get started:

1. Talk to your insurance agent about what they offer
2. www.debix.com

Web Sites referred to in presentation

online search engine to search your name
www.zabasearch.com
virus protection for your computer
Norton or McAfee Software Security Suite
to hold your mail
www.usps.com

Speaker Information:

Jeff Lanza
Phone: 816-853-3929
Email: jefflanza@thelanzagroup.com
Web Site: www.thelanzagroup.com

To sign up for my free newsletter, e-mail a request to:
jefflanza@thelanzagroup.com