Simple Safeguards:
Preventing Identity Theft

Presented by Retired FBI Special Agent Jeff Lanza

1. Protect Your Personal Information
- ✓ Don't carry your social security card.
- ✓ If asked to provide it – ask the person what law requires you to give your number and what happens if you refuse.

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.

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 or their attachments.

4. Protect Your Communications
- ✓ Make sure you have updated security software on your home computer.
- ✓ Don't conduct sensitive transactions on a computer that is not under your control.
- ✓ If you have wireless internet, make sure it is password protected.

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.

To remove your name from lists:
Mail - www.dmachoice.org; **Phone -** www.donotcall.gov
To stop preapproved credit card offers:
www.optoutprescreen.com ***or*** 1-888-5-OPTOUT (567-8688)
To hold your mail: www.usps.com

If a loved one dies:
- Send a copy of the death certificate to the three credit reporting agencies.
- Notify the Social Security Administration immediately.
- Don't mention a woman's maiden name or exact birth date in the obituary.

Speaker Information: Jeff Lanza
Phone: 816-853-3929
Email:jefflanza@thelanzagroup.com
Web Site: www.thelanzagroup.com
Send me an E-mail to get my free newsletter

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
- *To place a **fraud alert** on your account with all three credit reporting agencies:* www.fraudalerts.equifax.com
- You are allowed 3 free reports each year; to order: On Web: www.annualcreditreport.com By Phone: 1-877-322-8228

Terms to Understand:

1. **Fraud Alert:** Your credit file at all three credit reporting agencies is flagged and a potential lender should takes steps to verify that you have authorized the request.
   Inside Scoop: *Fraud alerts only work if the merchant pays attention and takes steps to* verify the identity of the applicant. *They expire in 90 days unless you have been a victim of identity theft, in which case you can file an extended alert - it lasts for seven years.*
2. **Credit Monitoring:** Your credit files are monitored by a third party - if activity occurs you are notified.
   Inside Scoop: *Talk to your insurance agent about what they offer. It is most likely the least expensive way to protect you and your family. You might consider* www.debix.com *– it has a comprehensive protection plan.*
3. **Credit Freeze:** A total lockdown of new account activity in your name. This requires unfreezing before you can open an account.
   Inside Scoop: A proven way to protect against identity theft. However, it can be cumbersome to start and stop. Credit freeze laws vary by state. To check your state go to: www.consumersunion.org

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

Simple Safeguards:
Preventing Fraud

Presented by Retired FBI Special Agent Jeff Lanza

Ten Tips to Avoiding Telemarketing Fraud:

It's very difficult to get your money back if you've been cheated over the phone. Before you buy anything by telephone, remember:

1. Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
2. Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware -- not everything written down is true.
3. Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state Attorney General, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.
4. Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
5. Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.
6. Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
7. It's never rude to wait and think about an offer. Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor.
8. Never respond to an offer you don't understand thoroughly.
9. Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.
10. If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.

Eight Tips to Avoid Health Insurance Frauds

1. Never sign blank insurance claim forms.
2. Never give blanket authorization to a medical provider to bill for services rendered.
3. Ask your medical providers what they will charge and what you will be expected to pay out-of-pocket.
4. Carefully review your insurer's explanation of the benefits statement. Call your insurer and provider if you have questions.
5. Do not do business with door-to-door or telephone salespeople who tell you that services of medical equipment are free.
6. Give your insurance/Medicare identification only to those who have provided you with medical services.
7. Keep accurate records of all health care appointments.
8. Know if your physician ordered equipment for you.

Five Tips to Avoiding Counterfeit Prescription Drugs

1. Be mindful of appearance. Closely examine the packaging and lot numbers of prescription drugs and be alert of any changes from one prescription to the next.
2. Consult your pharmacist or physician if your prescription drug looks suspicious.
3. Alert your pharmacist and physician immediately if your medication causes adverse side effects or if your condition does not improve.
4. Use caution when purchasing drugs on the Internet. Do not purchase medications from unlicensed online distributors or those who sell medications without a prescription. Reputable online pharmacies will have a seal of approval called the Verified Internet Pharmacy Practice Site (VIPPS), provided by the Association of Boards of Pharmacy in the United States.
5. Product promotions or cost reductions and other "special deals" may be associated with counterfeit product promotion.

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

Cyber Fraud
Preventing Account Takeovers

Presented by Retired FBI Special Agent Jeff Lanza

Problem: Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered. Where cyber criminals once attacked mostly large corporations, they have now begun to target municipalities, smaller businesses, and non-profit organizations. Thousands of businesses, small and large, have reportedly fallen victim to this type of fraud.

Source: FBI

How it is Done:

Cyber criminals will often "phish" for victims using mass emails, pop-up messages that appear on their computers, and/or the use of social networking and internet career sitess. For example, cyber criminals often send employees unsolicited emails that:

- ✓ Ask for personal or account information;
- ✓ Direct the employee to click on a malicious link provided in the email; and/or
- ✓ Contain attachments that are infected with malware.

Cyber criminals use various methods to trick employees into opening the attachment or clicking on the link, sometimes making the email appear to provide information regarding current events such as natural disasters, major sporting events, and celebrity news to entice people to open emails and click. Criminals also may disguise the email to look as though it's from a legitimate business. Often, these criminals will employ some type of scare tactic to entice the employee to open the email and/or provide account information. For example, cyber criminals have sent emails claiming to be from:

1. UPS (e.g., "There has been a problem with your shipment.")
2. Financial institutions (e.g., "There is a problem with your banking account.")
3. Better Business Bureaus (e.g., "A complaint has been filed against you.")
4. Court systems (e.g., "You have been served a subpoena.")

Crooks may also use email addresses or other credentials stolen from company websites or victims, such as relatives, co-workers, friends, or executives and designing an email to look like it is from a trusted source to entice people to open emails and click on links.

Detect

- ✓ **Monitor and reconcile accounts at least once a day.**
- ✓ **Discuss the options offered by your financial institution to help detect or prevent out-of-pattern activity.**

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

What You Can Do to Keep Safe - Education

Educate everyone on this type of fraud scheme

- Don't respond to or open attachments or click on links in unsolicited e-mails. If a message appears to be from your financial institution and requests account information, do not use any of the links provided.
- Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem, as it could actually be malicious software that allows the fraudster to remotely access and control your computer.

What You Can Do to Keep Safe - Computers

Enhance the security of your computer and networks to protect against this fraud.

1. Conduct online banking and payments activity from at least one dedicated computer that is not used for other online activity.
2. Do not leave computers with administrative privileges and/or computers with monetary functions unattended. Log/turn off and lock up computers when not in use.
3. Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
4. Install routers and firewalls to prevent unauthorized access to your computer or network.
5. Change the default passwords on all network devices.
6. Install security updates to operating systems and all applications, as they become available.
7. Block pop-ups.
8. Keep operating systems, browsers, and all other software and hardware up-to-date.
9. Do not use public Internet access points (e.g., Internet cafes, public Wi-Fi hotspots (airports), etc.) to access accounts or personal information. If using such an access point, employ a Virtual Private Network (VPN)

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

Simple Safeguards:
Preventing Social Media Fraud

Presented by Retired FBI Special Agent Jeff Lanza

Keep your guard up on sites like Facebook, LinkedIn and Twitter. Scammers are exploiting the trust we have of our connections on these sites to gain access to your accounts and commit fraud.

Current Threats

Fake Notification E-mails

Look out for fake emails that look like they came from Facebook. These typically include links to phony pages that attempt to steal your login information or prompt you to download malware. Never click on links in suspicious emails. Log-in to a site directly.

Suspicious Posts and Messages

Wall posts or messages that appear to come from a friend asking you to click on a link to check out a new photo or video that doesn't actually exist. The link is typically for a phony login page or a site that will put a virus on your computer to steal your passwords.

Money Transfer Scams

Messages that appear to come from friends or others claiming to be stranded and asking for money. These messages are typically from scammers. Ask them a question that only they would be able to answer. Or contact the person by phone to verify the situation, even if they say not to call them.

General Online Safety Rules

- **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives. If you interact with strangers, be cautious about the amount of information you reveal or agreeing to meet them in person.
- **Be skeptical** - People may post false or misleading information about various topics, including their own. Try to verify the authenticity of any information before taking any action.
- **Evaluate your settings** - Use privacy settings. The default settings for some sites may allow anyone to see your profile. Even private information could be exposed, so don't post anything that you wouldn't want the public to see.
- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

Security Information For Social Networking Sites

www.facebook.com/security
www.twitip.com/twitter-security-dos-and-donts
www.linkedin.com/secure/settings

Specific Actions to Avoid

1. **Don't click on a message that seems weird.** If it seems unusual for a friend to write on your Wall and post a link, that friend may have gotten phished.
2. **Don't enter your password through a link.** Just because a page on the Internet looks like Facebook, it doesn't mean it is. It is best to go the Facebook log-in page through your browser.
3. **Don't use the same password on Facebook that you use in other places on the web.** If you do this, phishers or hackers who gain access to one of your accounts will easily be able to access your others as well, including your bank.
4. **Don't share your password with anyone.** Social sites will never ask for your password through any form of communication.
5. **Don't click on links or open attachments in suspicious emails.** Fake emails can be very convincing, and hackers can spoof the "From:" address so the email looks like it's from a social site. If the e-mail looks weird, don't trust it, and delete it from your inbox.
6. **Don't send money anywhere** unless you have verified the story of someone who says they are your friend or relative.
7. **Don't provide your cell phone number to verify the results of a Facebook game or survey without reading the terms and conditions**. It may result in recurring charges on your cell phone bill.

More resource Information:

www.us-cert.gov *or* **www.fbi.gov**

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