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.
- ✓ Don't provide your social security number to anyone unless there is a legitimate need for it.

2. Protect Your Documents
- ✓ Shred your confidential trash with a cross-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 open their attachments.
- ✓ Don't click on links in e-mails from unknown senders.

4. Protect Your Communications
- ✓ Keep your computer and security software updated
- ✓ Don't conduct sensitive transactions on a computer that is not under your control.
- ✓ Protect your Wi-Fi with a strong password and WPA2 encryption.

5. Check Your Credit Report
- ✓ Order your free credit reports three times per year.
- ✓ Check financial accounts often for any unusual activity.

General Rules For Computer Security:
- If you did not go looking for it, then don't download it.
- If you did download it, then update it when asked.
- Don't click on links in emails from unknown senders.
- Be cautious when clicking on links in emails from known senders as their account may have been hijacked.

Identity Theft for Tax Related Purposes

If you are the victim of identity theft, or at risk because your information has been breached, go to: www.irs.gov and follow the instructions to fill out form 14039.

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)

Password Managers and Anti-Virus Protection

A popular and effective program for removing malware is called Malwarebytes; Popular password management programs include: Keeper; LastPass; Dashlane;

Speaker Information: Jeff Lanza
Phone: 816-853-3929
Email:jefflanza@thelanzagroup.com
Web Site: www.thelanzagroup.com
Send me an E-mail to receive a PDF file of this handout

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.allclearid.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
Craigslist Safety: **www.craigslist.org/about/scams**
EBay Security: **www.pages.ebay.com/securitycenter**

Protecting Your Family in The Information Age

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
Watch 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.

See What Others Can Find About You Online
www.zabasearch.com
www.spokeo.com
www.socialmention.com
www.topsy.com

Security Information For Social Networking Sites
www.facebook.com/security
twitter.com/settings/security
www.linkedin.com/secure/settings

Snapchat Users:

Users should be aware that there are apps that can be downloaded that will automatically record a copy of the Snapchat message - regardless of how quickly the message disappears after opening. Many of the image saving apps take a screen shot of the Snapchat message without any notification being provided to the sender.

Key Resources:

To Report Internet Fraud: www.ic3.gov
FBI (202) 324-3000 or your local field office
Craigslist Safety: **www.craigslist.org/about/scams**
EBay Security: **www.pages.ebay.com/securitycenter**

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.

Social Networking Security Reminders

1. Sign out of your account after you use a publicly shared computer.
2. Don't put your email address, address or phone number in your profile.
3. Only connect to people you know and trust.

Controlling Your Visibility on Instagram

How to set your photos and videos to Private:

Tap **"Edit Your Profile"**
iPhone/iPad: Scroll down to **"Posts Are Private"** and toggle the switch to **On**

Android or **Windows Phone**: Check the box next to **"Posts are Private"**

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

Simple Safeguards:
Information Protection 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**

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 sites[5]. 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.

They may also use variations of email domains that closely resemble the company's domain and may go unnoticed by the recipient who is being requested to make the transfer.

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

Businesses May Absorb Losses!

The Uniform Commercial Code does not require banks to refund money lost by fraudulent transfer.

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.

Preventing Wire Transfer/ACH Fraud

1. Conduct online banking and payments activity from one dedicated computer that is not used for other online activity.
2. Use all bank provided wire transfer controls
3. Require two persons to consummate all wire transfers to external parties.
4. Require the bank to talk to someone at your organization before the wire transfer is consummated.
5. Restrict the bank accounts from which a wire transfer can be made.
6. Any wire transactions over a set high dollar amount must have the approval of the business owner/CEO.
7. Use unique passwords or a bank supplied token to access wire-transfer software.
8. Review daily bank account activity on a regular basis.
9. Require sufficient documentation and have a second person review all wire transfer journal entries.
10. Establish positive pay and block for ACH transactions. This will eliminate the possibility of non-approved transactions.

Simple Safeguards:
Preventing Fraud Against Businesses

Presented by
FBI Special Agent Jeff Lanza
(Retired)

Five Common Scams That Target Businesses of All Sizes

1. **Phishing E-mails** – Phishing e-mails specifically target business owners with the goal of hacking into their computer or network. Common examples include e-mails pretending to be from the IRS claiming the company is being audited or phony e-mails from the Better Business Bureau, saying the company has received a complaint. If you receive a suspicious e-mail like this, don't click on any links or open any attachments.
2. **Data Breaches** – No matter how vigilant your company is, a data breach can still happen. Whether it's the result of hackers, negligence or a disgruntled employee, a data breach can have a severe impact on the level of trust customers have in your business. Educate employees on the importance of protecting information and practice the "need to know policy" internally.
3. **Directory Scams** – Commonly the scammer will call the business claiming they want to update the company's entry in an online directory or the scammer might lie about being with the Yellow Pages. The business is later billed hundreds of dollars for listing services they didn't agree to.
4. **Overpayment Scams** –If a customer overpays using a check or credit card and then asks you to wire the extra money back to them or to a third party, don't do it. This is a very popular method to commit fraud. Wait until the original payment clears and then offer the customer a refund by check or credit.
5. **Phony Invoices** – The United States Postal Service suspects that the dollar amount paid out to scammers as a result of phony invoices may be in the billions annually, mostly from small and medium sized businesses. Scrutinize invoices carefully and conduct regular audits of accounts payable transactions.

A pre-employment background investigation should include checks and verifications in the following areas:

- Employment history; Education;
- Professional accreditation;
- Military record;
- Credit history; Motor vehicle record;
- Arrests; Workplace violence or threatening behavior;

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

Preventing Check Fraud

- Use Positive Pay, the annual cost of which is far below the cost of **one** average check fraud case.
- Use secure checks, which include many features to prevent different types of check fraud.
- Securely store check stock, deposit slips, bank statements and cancelled checks.
- Implement a secure financial document destruction process using a high security shredder.
- Establish a secure employee order policy for check stock.
- Purchase check stock from established vendors.
- Regularly review online images of cancelled checks.

Preventing Embezzlement

Things You Should Do:

1. Separate duties and powers with regard to payments and account reconciliation.
2. Establish a tips hotline that offers anonymity and the possibility of a reward.
3. Conduct surprise audits as employees may be able to cover-up some fraud in advance of an audit.
4. Never completely trust anyone – many large fraud cases have been undertaken by "a most trusted employee".

Watch Out When an Employee:

1. Doesn't want to take a day off.
2. Makes expensive purchases including luxury items, cars, boats, exotic vacations and second homes.
3. Has high personal debt, high medical bills, poor credit, personal financial loss and addictions.

Red Flags That May Signal Integrity Issues

Cynicism; Alienation from coworkers; Poor or inconsistent work performance; Resentment of management; Behavioral changes or work habit changes; Employee sense of entitlement;

To Promote an Ethical Workplace

- Demonstrate top management commitment.
- Communicate expectations on a regular basis.
- Maintain focus on vision and mission.
- Monitor conduct – trust but verify.
- Maintain whistleblower channels and policies.
- Respond quickly to misconduct.
- Reward acts of integrity.