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.
- ✓ Be aware that most Medicare cards use the social security number as the Medicare number. Take steps to protect your card.

2. **Protect Your Documents**
- ✓ Shred your sensitive trash with a cross-cut or micro-cut shredder.
- ✓ Don't leave outgoing mail with personal information in your mailbox for pickup.

3. **Be Vigilant Against Tricks**
- ✓ Never provide personal information to anyone in response to an unsolicited request.
- ✓ Never reply to unsolicited emails from unknown senders or open their attachments.
- ✓ Don't click on links in emails 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. **Protect Your Digital World**
- ✓ Use strong passwords with at least eight characters including upper and lower case, numbers and symbols.
- ✓ Use different passwords for your various accounts.
- ✓ If you store passwords in a file on your computer, encrypt the file when you save it and assign a strong password to protect that file. This sounds obvious, but, don't name the file "passwords".
- ✓ Consider using password management programs.

Social Networking Security Reminders

1. Login directly, not through links.
2. Only connect to people you know and trust.
3. Don't put your email address, physical address, or phone number or other personal information in your profile.
4. Sign out of your account after you use a public computer.

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 this site: https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft

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)

Speaker Information: Jeff Lanza

Phone: 816-853-3929

Email:jefflanza@thelanzagroup.com

Web Site: www.thelanzagroup.com

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 take 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
Identity Theft Resource: www.identitytheft.gov
Craigslist Safety: **www.craigslist.org/about/scams**

Protecting Your Family in The Information Age

Presented by Retired FBI Special Agent Jeff Lanza

Never go to a login in page through a link in an email or a pop up. Always go to the login page directly by typing the site name or, preferably, through a stored bookmark that you created.

General Rules for Computer Security:

- If you were not looking for it, then don't download it.
- Keep your software current with the latest updates.
- 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.
- Keep your Windows computer protected with anti-virus software that comes with current Windows software or use third party software such as Norton or McAfee.
- Use CLT+ALT+DEL to exit a popup safely in Windows.

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. Login 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.
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.

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

Popular Programs:

Malware Removal: Malwarebytes.
Password Management: Keeper, LastPass, Dashlane.

Specific Actions to Avoid

1. **Don't click on a message that seems weird.** If it seems unusual for a friend to post a link, that friend may have gotten their site hijacked.
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 login 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 may be able to access your other accounts as well, including your bank.
4. **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. Delete it.
5. **Don't send money anywhere** unless you have verified the story of someone who says they are your friend or relative.

Ransomware aka Cryptowall

This fraud scheme begins when the victim clicks on an infected advertisement, e-mail, or attachment, or visits an infected website. Once infected with the ransomware, the victim's files become encrypted. In most cases, once the victim pays a ransom fee, they regain access to the files that were encrypted. ***Here are three ways to stay protected:***
Educate computer users about clicking on suspicious links or popups. Sometimes these come in the form of a package delivery notification from major brand names like Amazon, FedEx or UPS.
Enable popup blockers. Popups are regularly used by criminals to spread malicious software.
Always backup the content on your computer. If you are infected by ransomware, you can have your system wiped clean and then restore your files from your back up. Also, because ransomware can infect all hard drives, disconnect the backup drive when not in use or use cloud backup.

Password Management

Try to use different strong passwords for all your accounts. At a minimum, have different passwords for multiple email accounts, social networking, financial and employer sites.

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