Protecting Your Family in The Information Age (2018)

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 PC protected with Windows Defender or antivirus software from a third party.
- Use CTL+ALT+DEL to exit a popup safely in Windows.
- Use CMD+Option+Escape to exit a popup on a Mac.

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.

Two Factor Authentication

Requires you to provide a password **and** a PIN code (most often sent to your phone) to log in to online accounts. Use this to prevent hijacking of your accounts. In most cases you can set this up in the "settings" section of your account.

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