

Simple Safeguards: How to Stay Safe From Identity Theft and Cybercrime

Presented by Retired
FBI Special Agent Jeff Lanza
jefflanza@thelanzagroup.com;
www.thelanzagroup.com

About the presenter: Jeff was an FBI Special Agent for over 20 years, during which he investigated cybercrime, organized crime, human trafficking, and terrorism. Jeff has lectured at Harvard and Princeton Universities and written two highly reviewed books. He is featured in a Netflix documentary about the FBI and he often appears on national television news programs where he talks about the growing threat of cybercrime.

Here's an executive summary of the presentation with more details on the following pages:

1. Prevent Identity Theft

Create an online social security account

With your social security number and other personal information, a criminal can sign-up for social security benefits in your name and have the benefits sent to them. Here is what to do: If you are 62 years-of-age or older and have not created your online social security account, prevent a criminal from doing it before you. Sign-up at www.ssa.gov.

Freeze your four credit reports

A freeze restricts access to your credit reports and should prevent new accounts from being opened in your name. You will have to lift the freezes before you can open a new account. Freezing is highly recommended and is a proven way to protect against new account fraud. To freeze your credit reports, see the contact information of the reporting agencies on the next page.

Protect your information

Shred your sensitive trash with a cross-cut, micro-cut or diamond-cut shredder. Don't leave outgoing mail with personal information in your mailbox for pickup. Consider signing-up for e-delivery of all your financial statements, as this is the more secure way to have documents delivered. Be wary of unsolicited phone calls, text messages and emails. You should not provide your social security number or money to people who contact you in an unsolicited fashion.

2. Watch Out for Tricks

Account takeovers

As the term implies, account takeovers happen when someone gets unauthorized access to your online accounts. To prevent this, don't click on links or attachments in emails that you were not expecting or that don't make sense. Always log in to accounts by going directly to their websites, not through links.

Wire transfer fraud

This occurs when a criminal tricks a victim into wiring money to their bank account. Most commonly, a real estate company's email account is hijacked by a hacker, which provides them with information about people who are about to close on a home purchase. Right before closing, the hacker sends an email from the hijacked account to the home buyer instructing them to wire money for the closing to the criminal's or a mule's bank account. It can be very difficult to recover this money if it is not discovered very quickly. It is important to verify wire transfers with the recipient by phone or in person before sending money.

Ransomware

Beware of pop-ups and attachments in emails that could lock your computer or files. The criminal then demands a ransom to provide a key to unlock them. Also, backup your important files on a removable drive and in the cloud.

3. Protect Your Computer

Beware of pop-ups

Be cautious of pop-ups. Examples include ones that say you have to download something to see a video or a message that says there are threats detected on your computer. Don't click on anything in these pop-ups, including the "X" inside the pop-up itself. To remove the pop-up safely, hold down three keys: CTL+ALT+DEL (Windows) or CMD+Option+Escape (Mac). Then run your antivirus software to see if there is malware on your computer that caused the pop-up.

Update and back up

To stay safe from the latest threats, make sure that your operating system software and antivirus software is updated. Also, back up your files on a regular basis so you can recover if affected by a ransomware attack.

Use passphrases instead of passwords

A passphrase is composed of a combination of words strung together. Passphrases protect us against two hacks the criminals use to gain access to our accounts. First, **brute force attacks**, where hackers use powerful programs and computers to guess passwords. Second, **credential stuffing**, where a hacker obtains a password for one site and uses it to hack another site. It's a two for one special! Strong passwords will also keep us safe against these threats, if you use a different one for each account, which unfortunately, not all of us do. See page four in this document for more information about passphrases.

Preventing Identity Theft

Protect Your Social Security Number

- ✓ Don't provide your social security number to anyone unless there is a legitimate reason, which include occasions when you are applying for employment, opening a financial account, freezing your credit reports or if someone is conducting a background investigation on you. Your doctor does not require your social security number for medical services.
- ✓ The Social Security Administration does not contact people by phone. If you receive a phone call purporting to be from them, it is most likely a trick to get you to provide your social security number.
- ✓ Don't routinely carry your social security card or any document on which it is printed with you.
- ✓ If someone that you contact asks you to verify the last four digits of your social security number, that's okay.

If a criminal steals an identity, here are six things they can do - and how you can stay safe:

① They open credit card accounts, bank accounts and loans in your name.

Prevention: Freeze all four of your credit reports. A freeze restricts access to your credit reports and should prevent new account activity in your name. Once frozen, you must lift the freeze before you can get new credit. Freezing is highly recommended and is a proven way to protect against new account fraud. Below is the contact information for the agencies.

Experian: (888) 397-3742 | P.O. Box 9530 Allen, TX 75013 | www.experian.com/freeze

Equifax: (800) 685-1111 | P.O. Box 740241 Atlanta, GA 30374 | www.equifax.com/personal/credit-report-services

Innovis: (800) 540-2505 | P.O. Box 1640 Pittsburgh, PA 15230 | www.innovis.com/personal/securityfreeze

Trans Union: (888) 909-8872 | P.O. Box 2000 Chester, PA 19016 | www.transunion.com/credit-freeze

Keep your credit reports frozen indefinitely. You can freeze credit reports by mail, phone or online. It's easiest to do it online. When freezing, you will create a PIN, which is needed to lift the freeze when necessary.

Before you freeze your credit reports, it's a good idea to check them for unusual activity.

You are allowed four free reports each year. To order three: www.annualcreditreport.com or 877-322-8228; Your credit report at Innovis must be ordered from: www.innovis.com/personal/creditreport

② They file state and federal tax returns in your name.

Prevention: For federal taxes, depending on where you live, you might be able to get a PIN from the IRS to prevent fraud. To see if you can, go to this site: www.irs.gov. Check with your state authorities to see what methods they use to help prevent fraud. Victims won't be able to file tax return in the normal manner. But they still must pay their tax on time!

③ They get medical care or prescription drugs in your name.

Prevention: Notify your medical insurance provider if you have been a victim of any other form of identify theft. Check your health insurance statements carefully. If a criminal uses your identity to receive medical services, not only does it defraud the insurance provider, but it could create entries in your permanent medical record for procedures you did not receive and conditions that you don't have.

④ They file for social security benefits in your name (if you're eligible.)

Prevention: Create an online social security account at www.ssa.gov. When you create an online account, it does not mean that you have to collect benefits, just that a criminal can't do that in your name. Note that you can create your online account at any age and track your benefits throughout your lifetime through this online portal.

⑤ They file for unemployment benefits using your identity.

Prevention: There has been a large increase in fraudulent unemployment claims using stolen identities. Criminals filing for benefits using a stolen identity must have the personal information of the victim. It is important to be wary of telephone calls, text messages, letters, non-verified websites, or emails that require you to provide sensitive information, including birth dates and social security numbers. If you have become a victim, contact your employer and your state unemployment office to report the fraud and follow their instructions regarding resolution.

⑥ They steal the identity of a deceased person

Prevention: Identity theft could happen after someone dies. A criminal may use a deceased person's details to drain accounts, set up new loans, steal government benefits and more. Here is what you should do: Get copies of the official death certificate and provide it to all four credit bureaus and the deceased's financial institutions.

Other terms regarding credit reports and what they mean:

Credit Monitoring: Your credit reports are monitored and if activity occurs, you are notified. *Inside Scoop: Credit monitoring does not prevent fraud. It only notifies you when your credit reports have been accessed. In most cases, the monitoring companies provide other benefits such as help with resolution, which can be very beneficial.*

Fraud Alert: Your credit file at the four credit reporting agencies is flagged for 90 days or for seven years if you have already had your identity stolen. Creditors should take steps to verify the identity of a person opening a new account. *Inside Scoop: Not worth the effort. Fraud alerts only work if the merchant takes steps to verify the identity of the applicant.*

Credit Lock: Limits access to your credit reports by some parties without your approval. *Inside Scoop: Don't use this. Locks are not governed by federal law, there is no guarantee of error free operation and some credit reporting agencies may charge you a monthly fee for this service.*

Steps to take if you are a victim of identity theft

1. Visit IdentityTheft.gov to report and recover from identity theft. This site should provide you with a good plan to recover based on your personal situation. You may also need to take the following steps, if they are not included in the plan.
2. Check your credit reports for accounts that have been opened in your name.
3. Notify those organizations of the fraud.
4. Freeze all four credit reports. You can freeze your reports by phone, mail or online.
5. Call your local police and file a report.
6. Call the Social Security Administration's fraud hotline at 800-269-0271.
7. Contact the Internal Revenue Service at 1-800-829-0433.
8. Contact your state taxing agency and follow their instructions to address the situation.
9. Notify any organization that has your money, including financial advisors.
10. Notify your medical insurance providers.

Child identity theft

A child's social security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live. Check for a credit report to see if your child's information is being misused. If it is, visit IdentityTheft.gov to report and recover from identity theft. Federal law allows you to create and freeze credit reports for children to keep them safe from potentially years of fraud.

Social media and identity theft

Personal information - Information such as your full name (including your middle name), date of birth, hometown, pet names, interests and hobbies, nature of work, and home or office address are just some of the personal details that people post on their profile. Criminals can use these details to commit fraud. Protect this information to limit the risk of identity theft.

Friend requests - You should only accept friend request from people that you know. Some requests come from attackers, who then may share malicious links that lead to malware or phishing sites.

Your posts - By default, Facebook tends to make everything you put on it's network public. One quick way to lock down everything you post is to set your default sharing option to **friends** and not **public**. When you make this change, only your approved friends see your posts.

Robocalls and identity theft

In many cases, robocalls are used to help facilitate identity theft. Be skeptical of your caller ID, as it could be spoofed by a criminal to make it look like the call is coming from a federal agency like the IRS or Social Security Administration. As a rule, don't give information to people who contact you by phone. To help to stop robocalls, you might consider **Robokiller**, a cell phone app and **Nomorobo**, which can be used for landlines connected to the internet.

Identity theft and home title fraud

Criminals use your identity to forge paperwork which transfers your real estate into their name. The transfer is not legitimate, because it is based on fraudulent documents. However, it is possible they could sell the property before the fraud is discovered. Your best defense here is to routinely monitor your property's records in the county. Check with your county to see if they offer automatic notification if there is a record change.

To remove your name from lists:

Mail - www.dmachoice.org Phone - www.donotcall.gov

To stop credit card offers and other solicitations:

www.optoutprescreen.com or 1-888-5-OPTOUT (567-8688)

Key Resources

Police or FBI: Search online for local number
FTC: 1-877-IDTHEFT; www.identitytheft.gov

To Report Internet Fraud: www.ic3.gov

Preventing Cybercrime

Here is some more information about the tips that I discussed in the presentation.

Protect Your Credentials

- To prevent account takeovers, it is important to protect your login credentials. Go to login pages directly, not through a link in an email or a pop-up.
- Before entering personal information, ensure you are on a secure site by looking for a lock icon at the beginning of the web address.
- Click on the lock to see a certificate, which verifies the authenticity of the site.
- For future access, store the site's web address in your browser's bookmarks or favorites.

Hover to Discover

- Email addresses can be spoofed. Hold your mouse without pressing the button (hovering) over a sender in an email to see the true sender. If the two email addresses are different, then someone may be trying to trick you.
- Hovering also works with website links, so you can see where the link will re-direct you to if you click on it.
- If you see two letters before the first single slash in a website link, those letters refer to a country where the website is located. A foreign country code could indicate possible fraud.
- To preview a link on a mobile device, press and hold the link.

Multi-Factor Authentication (MFA)

With MFA, you use a password **and** a PIN (most often sent to your phone) to log in to online accounts. This will help prevent an online account takeover. At a minimum, it should be used for financial accounts and email accounts. Most email providers won't ask for the code every time you log in if they recognize your computer and IP address.

Software and Security

- It is imperative that Windows computers be protected with antivirus software. Popular options are **McAfee**, **Norton** and **Windows Defender**, which comes free with Windows 10.
- Keep in mind that these programs provide one layer of perimeter security. If malware evades them, they most likely won't be able to remove it because they couldn't stop it in the first place.
- You might consider a malware removal program that does search and destroy missions. A popular free program that is very effective is called **Malwarebytes**. The free version compliments your antivirus program. It does not replace it.
- Configure your settings so that your operating system software and antivirus software is updated automatically.

Passphrases

A passphrase is like a password, only it's composed of a combination of words strung together. That makes them easier to create and remember. Here are some tips to make strong passphrases:

- Use at least twelve characters to protect against **brute force attacks**.
- Create a unique passphrase for each online account. This prevents **credential stuffing**.
- If a website makes you add complexity, you can add it to the passphrases that you have created.
- Here's an example passphrase for a Netflix account: *leavetheguntakethecannoli* 😊

Passwords/Passphrases Managers

- Consider using a password manager to help keep track of all your unique passphrases. Some good options are **Keeper**, **Dashlane**, **1Password**, **LastPass** and **Bitwarden**.
- Another option is entering the passphrases in the note app on your smartphone and locking the note. This protects the contents of the note but keeps them accessible to you.

Unsubscribing from Emails

If you receive unwanted emails from organizations that you are familiar with and/or have done business with, you should unsubscribe. Don't reply to or unsubscribe from spam because that notifies the sender that you have an active email address, which could result in more spam. Send these emails to your spam folder.

Mobile Security

- Always use a passcode to protect your mobile devices. This keeps the information and apps more secure.
- Watch out for trick text messages. Don't call, click or reply unless you have verified the sender's authenticity.
- Download apps only from trusted sources. Make sure you check ratings and reviews if they are available and read the app's privacy policy to see exactly what personal information it will have access to if you download it.
- Don't give apps more permissions than they need for their purpose.
- Keep your operating system and apps updated. You can set you device to do this automatically in settings.
- Turn off Wi-Fi and Bluetooth when not needed. They announce your presence and are trackable by anyone interested.
- Delete unused apps from your mobile devices as they may have permission to access your personal information. Here's how for an **iPhone**: settings-general-iPhone storage-delete. For an **Android**: Settings-apps-uninstall.

Home Wi-Fi Networks

- Change your Wi-Fi's default name to make it harder for hackers to know what type of router you have.
- Change the default username and password for your router. It's easy for hackers to guess it, especially if they know the manufacturer.
- Use a strong passphrase and WPA2 encryption.
- If you have children actively using Wi-Fi, you might have a separate router for them to keep **you** safer.

Virtual Private Network (VPN)

Using an unsecured public Wi-Fi network could expose your private information. A virtual private network, better known as a VPN, creates a secure connection between your computer and the websites you are visiting. It is a must for accessing sensitive information in a public Wi-Fi network. Check the reviews on VPN options and get one that encrypts **all** of your traffic. Don't have a VPN? Use the cellular network on your phone to connect to the internet instead of the public Wi-Fi network.

Common Cybercrime Scams

Below are some more details on some common cybercrimes and how you can stay safe.

Fake Emails

- Be careful where you click. Don't click on links or attachments in emails from an unknown sender, a suspicious sender or in emails that don't make sense.
- Remember that a friend's email account can become compromised and that attackers can "spoof" someone's email address to appear to be from anyone.
- Don't react emotionally to an email. The hackers count on this to overcome logic and common sense to try to convince us to make bad decisions.

Email Account Takeovers

It is very important to protect email accounts from hackers. If they get access to an email account, they can use it as a base for committing fraud that could affect more than one person or account. For example, they might be able to:

- Log in to other accounts if the victim uses the same username and password.
- Send malware or links to fake login pages to your contacts, who think the email is coming from you.
- Send wire transfer requests to a financial advisor.

Tech Support Scams

Tech support scammers lure you with a pop-up window that appears on your computer screen that looks like an error message from your operating system or antivirus software. The message warns of a security issue on your computer and provides a phone number to get help. They want you to pay for tech support you don't need or to fix a problem that doesn't exist. They often want payment by gift card because it can be hard to reverse. They may ask for remote access to your computer. If someone calls you with this schtick, hang up and if you get a pop-up as described, don't call the number in the pop-up.

Email Extortion Scams

According to the FTC, this scam has increased recently. In this scenario, the scammers lie and say they have access to your computer, webcam or have installed clever software to hack your files. They threaten to release personal information about you and your online habits if you don't pay them. But they may really know one of your old – or recent – passwords and they include it in the message to prove it. Most likely, this was obtained through a third party breach. When you see that, you know it's time to update your password on that account. If you get a message like this, don't engage with them and report the incident to the FTC at www.FTC.gov/Complaint.

Ransomware

What it is: Ransomware is a form of malware that restricts access to data by encrypting files or locking computers.

How it begins: Victims will open an email addressed to them and may click on an attachment that appears legitimate, like a notification of a missed package delivery. This may cause ransomware code to install on their computer.

What happens next: The malware encrypts files on a victim's computer. They see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key to unlock a computer or recover the files.

To stay safe: Don't download attachments from an unknown source. Back up your files. But because ransomware can attack backups, using a cloud backup that can restore to previous versions that are not encrypted is a good option.

Real Estate Wire Transfer Fraud

It begins when a criminal hijacks the email account of lawyers, real estate agents, title companies or lenders to get the details of real estate transactions about to close. Then, posing as a party to the transaction, the criminal will email a buyer with instructions on where to wire money for the closing. The buyer, who believes they have received legitimate instructions, will wire the money to the criminal. A wire transfer is almost impossible to reverse once completed. This crime is an epidemic and growing. Not buying a home? Warn family and friends who are. You might save them thousands of dollars in losses.

There is too much money at stake for you to make a mistake. Here are some tips to stay safe from this crime:

Know that wiring instructions rarely change and be very suspicious of last-minute wiring changes. During a real estate transaction, know the phone numbers of all the parties and know their voice. Get the wiring information in person or over a verified phone number. Finally, if your gut is telling you something is wrong, investigate. You are probably right.