



MILITARY FAMILIES LEARNING NETWORK

Identity Theft: How to Reduce Your Risk

<https://learn.extension.org/events/2326>

U.S. DEPARTMENT
OF DEFENSE





MILITARY FAMILIES LEARNING NETWORK

Connecting military family service providers
to research and to each other
through innovative online programming

www.extension.org/militaryfamilies

Sign up for webinar email notifications at www.extension.org/62831²



MILITARY FAMILIES LEARNING NETWORK

Connecting military family service providers
to research and to each other
through innovative online programming

Join the Conversation Online!





PERSONAL FINANCE

Military Families Learning Network

Join the Conversation Online!



MFLN Personal Finance



MFLN Personal Finance @MFLNPF



Military Families Learning Network



MFLN Group <https://www.linkedin.com/groups/8409844>



Today's Presenters

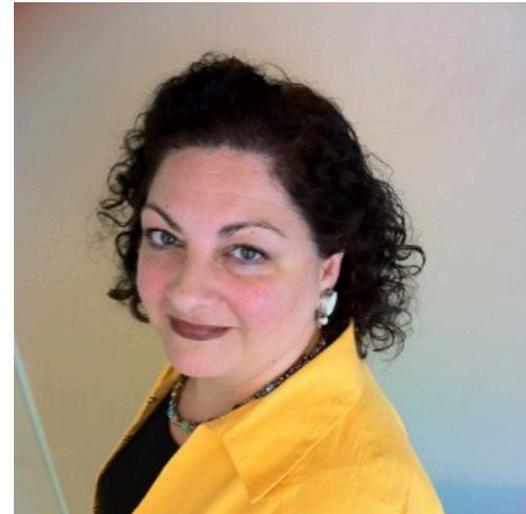
Dr. Barbara O'Neill

- Financial Resource Management Specialist for Rutgers Cooperative Extension
- Has been a professional, financial educator and author for more than 35 years.
- Has written more than 1,500 articles for academic journals, conference proceedings & other professional publications.



Carol Kando-Pineda

- Counsel in the FTC's Division of Consumer & Business Education
- She leads FTC teams to create and distribute free resources to help people spot, stop and avoid fraud, manage their money and make wise buys.
- She began her FTC career as a staff attorney bringing false advertising claims.



Question #1:

Has Anyone (or Family Member) Been an ID Theft Victim?

- Describe the situation
- Who was the fraudster (if known)?
- How was the case resolved?



Back in the Day....

What did people do when they wanted to steal a lot of money?



Some Famous Bank Robbers in U.S. History

- Bonnie and Clyde



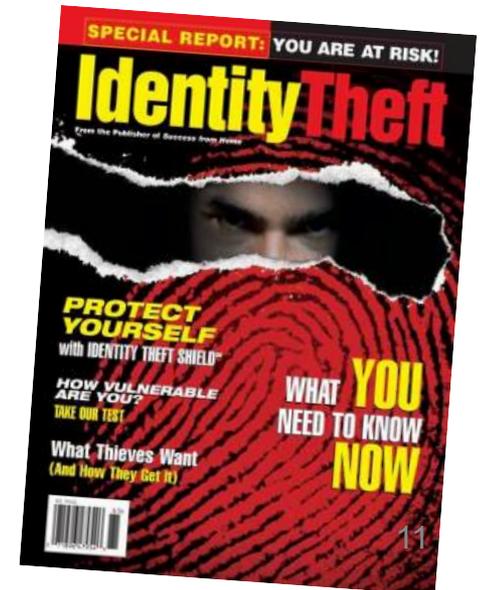
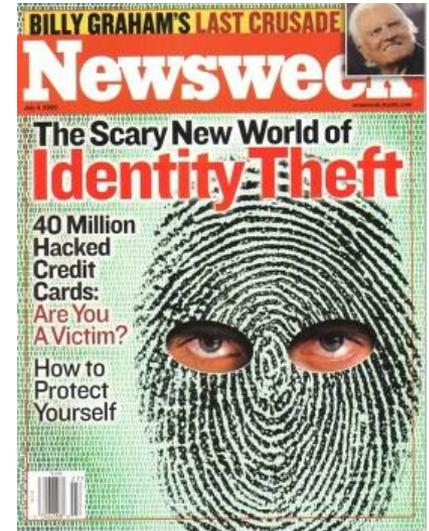
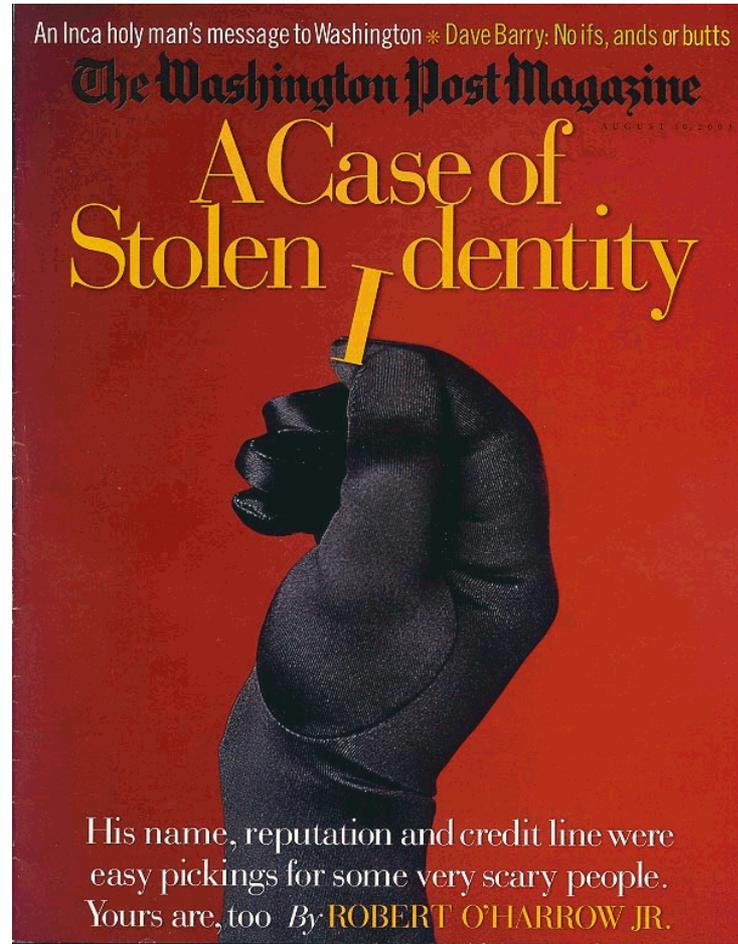
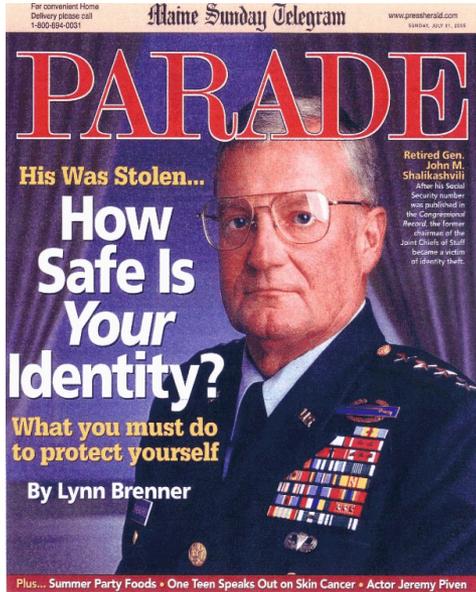
- John Dillinger



- Willie Sutton



Identity Theft Is in the News!



What Personal Information Is Stolen by Identity Thieves?



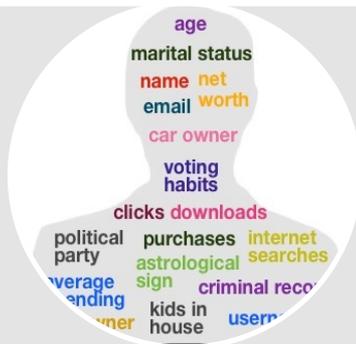
Name

Address

Date of birth

Social Security number (SSN)

Health insurance ID number



Mother's maiden name

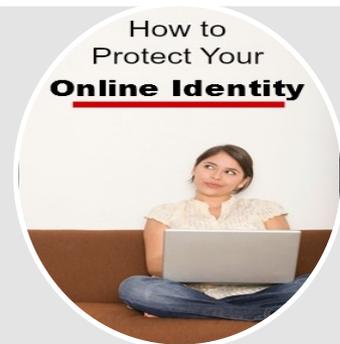
Username and passwords for web sites

Driver's license



Personal identification numbers (PINs)

Credit card information (numbers and expiry dates)



Bank account numbers

Signature

Passport number

Sources of Personal Information



1. You receive offers of pre-approved credit and, if you decide not to accept them, you do not shred them (10 points)
2. You carry your Social Security card (or other document with your SS number on it) in your wallet (10 points)
3. You do not have a post office box or a locked, secured mailbox (5 points)
4. You drop off your outgoing mail at an open, unlocked box or basket (10 points)
5. You have sensitive personal data posted online (e.g., a blog or social media) (10 points)

6. You do not shred or tear banking and credit information when you throw it in the trash (10 points)
7. You provide your Social Security number (SSN) whenever asked (20 points)
 - Add 5 points if you provide it orally without checking to see who might be listening
8. You are required to use your SSN as an employee or student ID number (5 points)
9. Your SSN is printed on an employee badge that you wear (10 points)
10. Your SSN or driver's license number is printed on your personal checks (20 points)

11. You are listed in a Who's Who Guide (5 points)
12. You carry an insurance card in your wallet and it contains your SSN or your spouse's SSN (20 points)
13. You have not ordered a copy of your credit report for at least two years (10 points)
14. You write checks with a "regular" pen instead of a gel pen with ink that cannot be "washed" (5 points)
15. You do not believe that people would root around in your trash looking for credit or financial information (10 points)

What Your Identity Theft Risk Score Means

- **100+ Points:** You are at HIGH RISK. You should purchase a paper shredder and become more security aware in document handling.
- **50-100 points:** Your odds of being victimized are about average; higher if you have good credit.
- **0-50 points:** Congratulations! You have a high security IQ. Keep up the good work.

FTC Identity Theft Video #1: How Identity Theft Happens

<http://www.youtube.com/watch?v=-IEBVIh7bzc>

DETER·DETECT·DEFEND
AVOID **THEFT**

FTC Identity Theft Video #2: Case Stories of Real People

<http://www.youtube.com/watch?v=OoPJImjP1ZQ>



Who are Identity Thieves?

- Narcotics users or sellers
- Organized crime and gangs
- Opportunists
- Desperate people
- Employees (business and government)
- Family members or someone close to you



Types of Identity Theft



Credit card fraud

Bank account fraud

Communications services fraud

Health insurance fraud

Fraudulent loans

Tax refund identity theft

Children's identity theft

Driver's license fraud

...and more!

Driver's License Identity Theft



- Your driving privileges could be suspended or revoked
- You could be arrested during a routine traffic stop for crimes you did not commit
- Thieves can open bank accounts, apply for credit, and cash checks in your name

Children's Identity Theft

http://today.msnbc.msn.com/id/42997608/ns/today-parenting_and_family/t/stop-id-thieves-stealing-your-kids-credit/



“I owe \$20,000 on four credit cards, my car was repossessed, and I turn two next month”



Criminals often use children’s identities, not for credit fraud, but to obtain a driver’s license, commit crimes, collect Social Security, and obtain medical treatment

Medical Identity Theft Video

<http://www.youtube.com/watch?v=EePx7STsnOI>



How Identity Theft Occurs

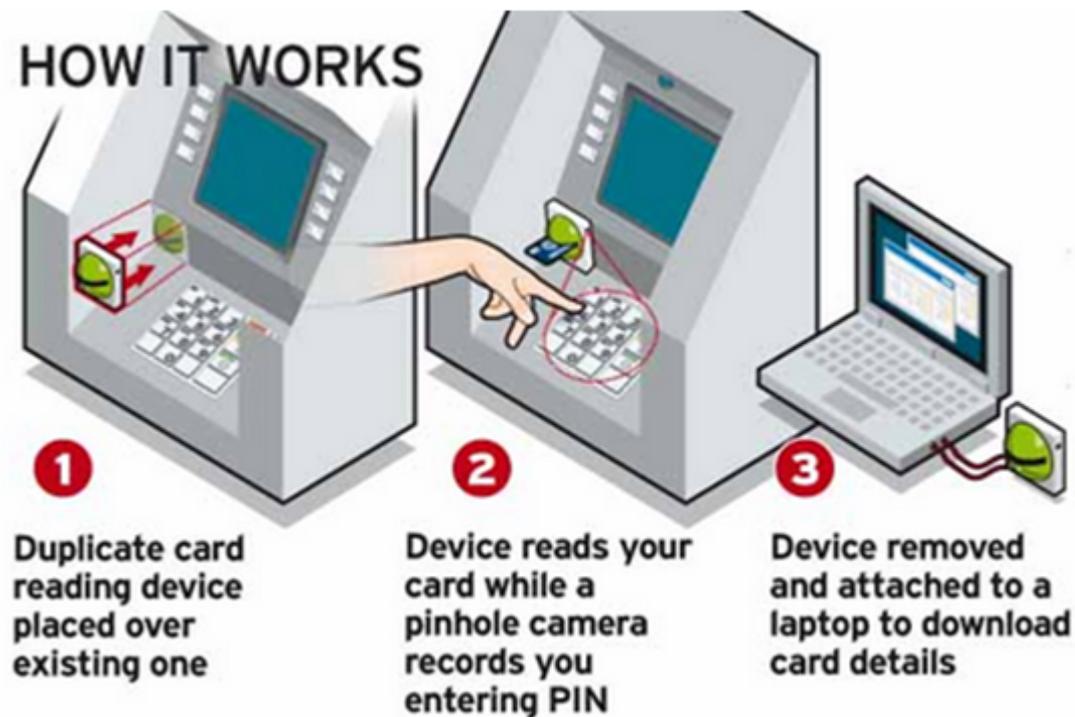
Identity thieves...

- steal wallets and purses containing your ID
- steal your mail
- rummage through trash (“dumpster diving”)
- pose fraudulently as someone else to get your information (“pretexting”)
- steal data with skimming devices



Skimming Machines

Skimming is stealing credit /debit card numbers with a device that reads and decodes information from the magnetic strip on the back of credit or debit cards



More Identity Theft Methods

Identity thieves...

- steal business or personnel records at your workplace
- find personal info in your home
- use info you put on the Internet
- buy personal info from “inside sources”
- “shoulder surf” at ATMs and telephones



Reducing Identity Theft Risk

- Destroy credit card applications, receipts, bank, and billing statements
- Avoid giving your SSN unless it's absolutely necessary -- use other identifiers
- Pay attention to billing cycles
- Guard your mail from theft
- Put passwords on smart phones
- Don't let your credit card out of your sight



More Ways to Reduce Identity Theft Risk

- Carry as little identification info as possible
- Limit the number of credit cards you carry
- Don't give personal identification info on the phone unless you initiate the call
- Be cautious with personal info in your home
- Check who has access to personal info at work
- Clean out your car

Still More Ways to Reduce Identity Theft Risk

- Don't carry your SS card
- Save ATM and credit card receipts to check against statements
- Alert family members to dangers of pretexting
- Make sure your credit reports are accurate
- Write checks with uniball gel pens



Technology Scams: Phishing, Fraudulent E-mails, etc.

```
00100101010100  
10010010000010  
01111010100000  
011PHISHING100  
11100101101001  
00100100100100
```

Look-Alike (Fake) Web Sites

- Spoof e-mail messages sent to “verify” or “update” account info
- Appears to come from reputable company
 - Example: eBay, Best Buy, banks, merchants
- Looks “legitimate”
- Scam is called “phishing”
 - Get people to disclose sensitive data
 - Data used to commit identity theft

00100101010100
10010010000010
01111010100000
011**PHISHING**100
11100101101001
00100100100100

Red Flags of a Phishing Scam

- E-mails that direct users to a Web site to “validate” or “update” info
- Threats that accounts will be closed
- Grammatical errors and typos
- Lack of a specific contact person, phone number, or address
- Words Like “Urgent” and “Immediately”

```
00100101010100  
10010010000010  
01111010100000  
011PHISHING100  
11100101101001  
00100100100100
```

Phishing Video: Symantic Guide to Scary Internet Stuff

<http://www.youtube.com/watch?v=K81WLwuiDwk>

00100101010100
10010010000010
01111010100000
011**PHISHING**100
11100101101001
00100100100100

Steps To Avoid Phishing

- Be cautious: African refugees with \$10 million, suspended FDIC insurance, etc.
- Realize that banks never ask for account info, especially in an e-mail
- Ditto for the IRS
- Don't click on any links in suspicious e-mails
- Report suspicious e-mails to companies and spam@uce.gov
- D-E-L-E-T-E

00100101010100
10010010000010
01111010100000
011**PHISHING**100
11100101101001
00100100100100

Phishing Sample #1

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of \$92.50. Please submit the tax refund request and allow us 3-6 days in order to process it. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click:
<http://easy-classifieds.com/Internal/Revenue/service/verify.html>

Regards, Internal Revenue Service

00100101010100
10010010000010
01111010100000
011**PHISHING**100
11100101101001
00100100100100

Phishing Sample #2

ATTN: An Iraqi made a fixed deposit of 44.5m usd in my bank branch and he died with his entire family leaving behind no next of kin,am ready to share 70/30 with you if you choose to stand as my deceased client next of kin.

Pls indicate by sending the following below to show your interest. 1.YOUR NAME 2.YOUR RESIDENT ADDRESS 3.YOUR OCCUPATION 4.YOUR PHONE NUMBER 5.DATE OF BIRTH 6.COUNTRY OF RESIDENT 7. ANY FORM OF YOUR IDENTIFICATION OR INTERNATIONAL PASSPORT

Your response with the requested information should be sent to reach me at my personal email address below: yi.simon19@gmail.com

Yours Truly, Simon Yi

00100101010100
10010010000010
01111010100000
011**PHISHING**100
11100101101001
00100100100100

Phishing Sample #3

Attention: Beneficiary I wish to use this medium and my office to inform you that your CONTRACT/INHERITANCE Payment of USD10,500,000.00 only from CENTRAL BANK OF NIGERIA has been RELEASED and APPROVED for onward transfer to you via ATM CARD which you will use in withdrawing your funds in any ATM SERVICE MACHINE in any part of the world, but the maximum you can withdraw in a day is USD\$10,000 Only.

The United States government has mandated the CENTRAL BANK OF NIGERIA, to send you the ATM CARD and PIN NUMBER. Therefore You are advised to contact the Head of ATM CARD Department of the CENTRAL BANK OF NIGERIA for further instructions on how to dispatch your ATM CARD to you.

Name: REV FR MARTINS UZOR DIRECTOR ATM DEPARTMENT OF CBN

Email: lap111@blumail.org

001001010100
10010010000010
01111010100000
011**PHISHING**100
11100101101001
00100100100100

Spear Phishing

- Instead of casting out thousands of random e-mails, spear phishers target victims more personally
 - May have stolen ID info
 - People that attend the same college OR use the same bank OR work for same employer, etc.
- E-mails to victims are more “personal,” which makes them dangerous and deceptive



Question #4: Do You Have Any Good Examples of Phishing Schemes?



2014 Study Findings

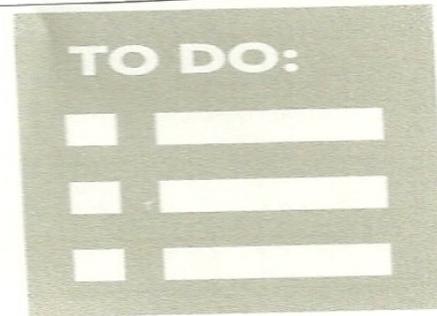


- The higher the score, the more frequently identity theft risk reduction practices are performed. The **mean quiz score** was **73.58** out of 100. Mean scores for individual quiz items ranged from 2.50 to 4.48 (1= Never, 5 = Always)
- **Two areas of weakness** were **checking one’s credit report annually** (2.65) and **securing incoming mail** (2.50).
- Almost two-thirds (64.4%) of respondents scored between 70 and 100. The three risk reduction strategies that were **performed most frequently** (mean score above 4) were **not divulging one’s SSN, not printing sensitive data on checks, and practicing “general security consciousness”**

New Resource: IdentityTheft.gov



Tell us what happened.



Get a recovery plan.



Put your plan into action.

Tax, medical & child identity theft and imposter scams

Carol Kando-Pineda
Federal Trade Commission

Tax Identity Theft

- Using someone else's Social Security number to file a fraudulent tax return

(or a deceased taxpayer's information to get their refund)
- Claiming someone else's children as dependents

Warning Signs

- Social Security number is lost, stolen, or compromised
- Unusual delay in getting a refund
- IRS notification:
 - duplicate tax return filing
 - unreported income

Immediate Steps for Victims

- Contact the IRS Identity Protection Specialized Unit at **800-908-4490** (8 a.m. to 8 p.m., local time)
- File **IRS Identity Theft Affidavit (Form 14039)**
- Have valid govt-issued identification
 - Social Security card, driver's license, or passport)
- When resolved, you'll get an Identity Verification PIN
- Go to: irs.gov/identitytheft

Immediate Steps for Victims

Step 1: Call the companies where you know fraud occurred

Call the fraud department

Explain that someone stole your identity

Immediate Steps for Victims

Step 2: Place a fraud alert and get your credit report

www.annualcreditreport.com or [1-877-322-8228](tel:1-877-322-8228).

Immediate Steps for Victims

Step 3: Report identity theft to the FTC

Complete the [online form](#) or call [1-877-438-4338](tel:1-877-438-4338). Include as many details as possible

Immediate Steps for Victims

Step 4: File a report with your local police department

Bring ID with photo, proof of address

MEMO FROM FTC TO LAW ENFORCEMENT

To: Law Enforcement Officer

From: Division of Privacy and Identity Protection
The Federal Trade Commission

Re: **Importance of Identity Theft Report**

The purpose of this memorandum is to explain what an “Identity Theft Report” is, and its importance to identity theft victims in helping them to recover. A police report that contains specific details of an identity theft is considered an “Identity Theft Report” under section 605B of the Fair Credit Reporting Act (FCRA), and it entitles an identity theft victim to certain important protections that can help him or her recover more quickly from identity theft.

Specifically, under sections 605B, 615(f) and 623(a)(6) of the FCRA, an Identity Theft Report can be used to permanently block fraudulent information that results from identity theft, such as accounts or addresses, from appearing on a victim’s credit report. It will also make sure these debts do not reappear on the credit reports. Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to allow an identity theft victim to place an extended fraud alert on his or her credit report.

In order for a police report to be incorporated in an Identity Theft Report, and therefore entitle an identity theft victim to the protections discussed above, the police report must contain details about the accounts and

Identity Theft Report



Preparing and Filing Tax Returns

- Know your tax preparer
- Mail tax returns as early in the tax season as possible

Preparing and Filing Tax Returns

- **Keep them safe:**
 - Not in outgoing mail
 - Secure network to transmit
 - Lock up copies
 - Shred, shred, shred

Preparing and Filing Tax Returns

- Minimize personal information in purses or wallets, or on smartphones
- Do not respond to unsolicited emails and calls that appear to be from the IRS

Medical Identity Theft

- Read every “Explanation of Benefits” statement you get from your health insurer
- Follow up on any item you don’t recognize
- Check your benefits

Medical Identity Theft

- Contact each doctor... or clinic, hospital, pharmacy, laboratory, and health plan where the thief may have used your information
- Get your records. Complete the providers' records request forms and pay any fees required to get copies of your records
- Check [your state's health privacy laws](#). Some state laws make it easier to get copies of your medical records

Medical Identity Theft

- Review your medical records, and report any errors to your health care provider
- Write to your health care provider to report mistakes in your medical records
- Notify your health insurer
 - Send your Identity Theft Report to your health insurer's fraud department
 - Tell them about any errors in your medical records

Child Identity Theft

- Follow the usual steps for [What To Do Right Away](#) and [What To Do Next](#) with 2 exceptions:
- Ask (phone or email) for a search based only on your child's Social Security number (SSN)
 - **Equifax**
[1-800-525-6285](tel:1-800-525-6285)
 - **Experian**
[1-888-397-3742](tel:1-888-397-3742)
 - **TransUnion.com**
childidtheft@transunion.com

Child Identity Theft

- Send each credit reporting agency the [Minor's Status Declaration \[PDF\]](#) form
 - It's proof that your child is a minor
 - Include a letter asking that all information associated with your child's name or SSN to be removed



IdentityTheft.gov



Tell us what happened.



Get a recovery plan.



Put your plan into action.



Report identity theft and get a recovery plan

Get Started →

or browse recovery steps

IdentityTheft.gov can help you report and recover from identity theft.

HERE'S HOW IT WORKS:



Tell us what happened.

We'll ask some questions about your situation. Tell us as much as you can.



Get a recovery plan.

We'll use that info to create a personal recovery plan.



Put your plan into action.

If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.



Which statement best describes your situation?

I want to report identity theft.



Someone else filed a tax return using my information.



My information was exposed in a data breach.



Someone got my personal information or my wallet, and I'm worried about identity theft.



Something else.





What did the identity thief use your information for?

Select all that apply

Credit card accounts

Telephone, mobile, or utility accounts

Debit, checking, or savings accounts

Employment or taxes

Government benefits or IDs

Loans or leases

Other account types (Internet, insurance, securities, medical, etc.)



1 Theft Details

2 Your Information

3 Suspect Information

4 Additional Information

5 Comments

6 Review Your Complaint

Report Identity Theft to the FTC

Next, we are going to ask for specific details. We will use the information you provide to create your:

Identity Theft Affidavit



Recovery Plan



This will help you fix problems caused by identity theft.

Continue →

How we handle your information

It's up to you to determine how much personal information you want to provide. The FTC enters this information into a secure online database that law enforcement agencies use in their investigations.

Please read our [Privacy Policy](#) to learn more about how we safeguard your personal information.

← Start Over



- 1 Theft Details
- 2 Your Information
- 3 Suspect Information
- 4 Additional Information
- 5 Comments
- 6 Review Your Complaint

Please review your identity theft affidavit.
 This is your official statement about what happened to you.

Edit

Identity Theft Victim's Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems.

About You (the victim)

(1) My full legal name: Jane Doe
First Middle Last Suffix

(2) My date of birth: 12/10/1973
mm/dd/yyyy

(3) My Social Security Number: _____ - ____ - _____

(4) My driver's license: _____

(5) My current street address:
123 Main Street Apt 23
Number & Street Name Apartment, Suite, etc.
Mapletown FL 12345 UNITED STATES
City State Postal Code Country

(6) I have lived at this address since: 7/15/2005
mm/dd/yyyy

(7) My primary phone: _____

Fill these items in by hand, after you print it out.

Leave (3) blank until you provide this form to someone with a legitimate business need, like when you are filing your report at the police station or sending the form to a credit reporting agency to correct your credit report.

← Previous

Finalize →



Your Report is not submitted yet.

Almost Done! We recommend creating a **free account** so you can:

- Get a **personal recovery plan** that tracks your progress
- Print **prefilled** letters & forms
- Return anytime to **update and view** your affidavit
- **Save time** if this ever happens again

Yes, submit and create account →

No thanks, submit without an account

I understand that I will **NOT** be able to make updates.

Instead, I will receive a **one-time copy** of my affidavit and recovery plan.



Welcome back.

Update your FTC Affidavit if you've discovered any new information.

[Yes, I have updates](#)

[Not Right Now](#)

Your Recovery Plan

[Print](#)

Resolve fraud dispute with Bank of America. [→](#)

You called 14 days ago. Did you get a confirmation letter yet?

Place a fraud alert on your credit report. [→](#)

File a report with your local police department. [→](#)

Correct your credit report. [→](#)

Consider adding an extended fraud alert or credit freeze. [→](#)

[Hide Completed Items \(1\)](#)

[✓ Report identity theft to the FTC.](#)



Identity Theft Report

This report proves to businesses that your identity was stolen.

[✓ Your FTC Affidavit](#)

[Update](#)

[Print](#)



[Your Police Report](#)

This is a paper document

[Add Police Report Info](#)



[Your Identity Theft Report](#)

This is a paper document

Imposter Scams

- On the rise
- Many variations on the hook....

Imposter Scams

Imposter complaints to FTC have skyrocketed

CY2013	126,000
--------	---------

CY2015	350,000
--------	---------

IRS complaints alone are up to 228,000

(from 64,000 in CY 2013)

The Great Pretenders

- The stories change but the ending is always the same...
 - IRS and Other government imposters
 - Online romance
 - Family emergency
 - Business/Tech support

Imposter Scams

- Scammers posing as the IRS call and say you owe taxes
- They might also:
 - know all or part of your SSN
 - rig caller ID to make it look like call is from DC (202 area code)

Imposter Scams

- **Imposters might:**

- threaten arrest or deportation
- demand immediate payment
 - pre-paid debit card or wire transfer
- send you bogus IRS emails to further the scheme

What you need to know

- **The IRS will not:**
 - ask you to pay with **prepaid debit cards or wire transfers**
 - ask for a **credit card number over the phone**
 - **threaten arrest**, deportation or loss of your drivers license
 - send you **emails** without prior contact

What you need to know

- If the IRS needs to contact you,
 - they **will first do it by mail**
- If you have any doubts,
 - call the IRS directly at **800-829-1040**

Military Consumer

Military.ncpw.gov

- July is month of the Military Consumer
- New toolkit coming soon

Questions?

Thank you!

Resources

[IdentityTheft.gov](https://www.identitytheft.gov)

[Consumer.FTC.gov](https://www.consumer.ftc.gov)

All our articles, videos, posts

[Consumer.gov](https://www.consumer.gov)

Just the basics

[FTC.gov/bulkorder](https://www.ftc.gov/bulkorder)

order any print materials for FREE!

What is *one significant thing* you learned today?

Key Takeaways

- Identity theft uses “no tech” and high tech methods
- Minimize the amount of information that can be stolen from you
- You cannot control every identity theft risk factor
- Identity theft is a crime that should be reported
- Act immediately to stop further use of your identity



Evaluation and Continuing Education Credits/Certificate of Completion

- MFLN Personal Finance is offering 1.5 credit hours for AFC-credentialed participants through AFCPE and CPFCs through FinCert.
- To receive a certificate of completion, please complete the evaluation and post-test at:
https://vte.co1.qualtrics.com/SE/?SID=SV_2aYT6lxWbYLzI2x
- Must pass post-test with an 80% or higher to receive certificate.

Personal Finance Upcoming Event

Life Insurance Basics for Military Families

- Date: April 5, 2016
- Time: 11 a.m.-12:30 p.m. Eastern
- Location:
<https://learn.extension.org/events/2496>

For more information on MFLN Personal Finance go to:

<https://blogs.extension.org/militaryfamilies/category/personal-finance/>



MILITARY FAMILIES LEARNING NETWORK

Find all upcoming and recorded webinars covering:

Personal Finance
Military Caregiving
Family Development
Community Capacity Building
Family Transitions
Network Literacy
Nutrition & Wellness

www.extension.org/62581

U.S. DEPARTMENT
OF DEFENSE

