

THE CHANGING FACE OF **IDENTITY THEFT**

**OWN YOUR
IDENTITY**

OR someone else **WILL!**

PRESENTED BY JOAN DYER, CITRMS

R **LEGAL**[®]
RESOURCES

THE CHANGING FACE OF **IDENTITY THEFT**

Agenda

- Background and statistics
- Prevention tips and warning signs
- What to do if identity theft happens to you

THE CHANGING FACE OF IDENTITY THEFT

Our perspective

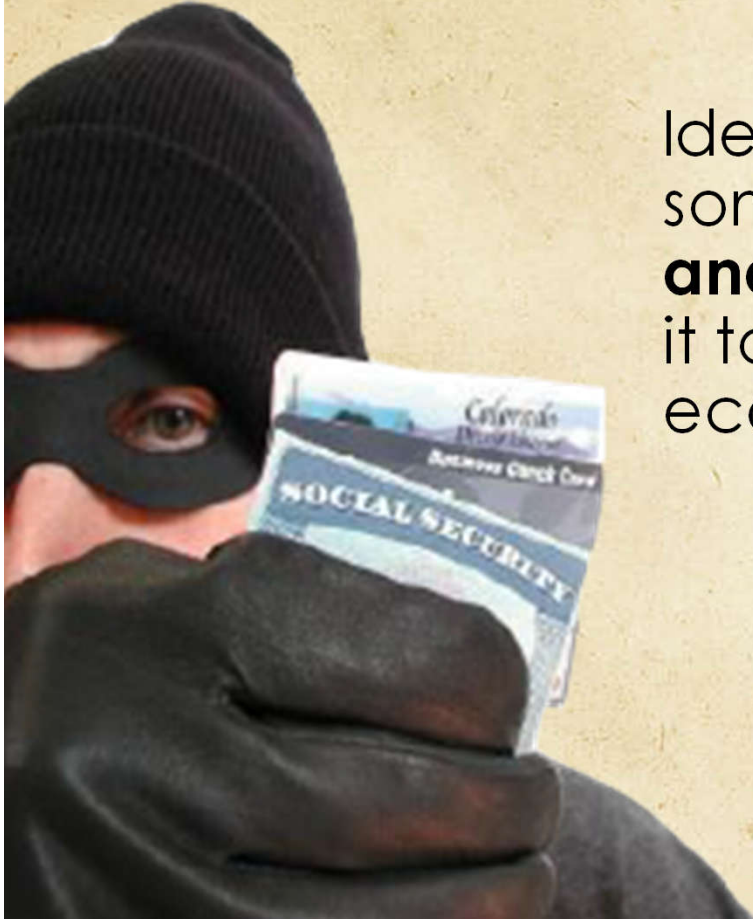
Legal Resources believes that ***education and constant vigilance*** are keys to **preventing** and ***managing the damages*** caused by identity theft.



THE CHANGING FACE OF IDENTITY THEFT

What is identity theft?

Identity theft is a crime in which someone **wrongfully obtains personal and/or financial information** and uses it to commit various types of fraud for economic or personal gain.



R LEGAL[®]
RESOURCES

THE CHANGING FACE OF IDENTITY THEFT

Startling Statistics

- Every **2 SECONDS** someone becomes a victim of ID theft
- **1 in 4 Americans** ages 16 or older have been a target or a victim of identity theft
- **\$17 BILLION** was stolen in 2017 by identity thieves
- **Tax- or wage-related fraud was the most common form of reported identity theft**, followed by credit card fraud, phone or utilities fraud, and bank fraud

THE CHANGING FACE OF IDENTITY THEFT

Startling Statistics

- **Michigan is the state with the highest per capita rate of reported identity theft complaints**, followed by Florida, Delaware, & California .
- New Account Fraud (32.7% of fraud) victims are **3x more likely** to take a year or more to discover that their identities were misused compared to other types of fraud.
- Equifax admits **147.9 million** Americans were exposed in the 2017 breach- *5 million more than first reported*. Estimating that more than half of the US population with Social Security numbers are at high risk.

THE CHANGING FACE OF IDENTITY THEFT

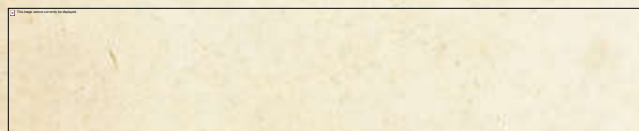
- W-2 Scams
- The W-2 form scam has emerged as one of the [most dangerous phishing emails](#) in the tax community. During the last two tax seasons, cybercriminals have tricked payroll personnel or people with access to payroll information into disclosing sensitive information for entire workforces.
- The scam affected all types of employers, from small and large businesses to public schools and universities, hospitals, tribal governments and charities. Incidents reported from victims and non-victims increased to 900 in 2017, compared to slightly over 100 in 2016. There are additional [tax scams](#) popping up constantly as well, including those targeting tax preparers.

THE CHANGING FACE OF IDENTITY THEFT

Recent Breaches of High Profile Companies



STAPLES



THE CHANGING FACE OF IDENTITY THEFT

The Identity Theft Resource Center (ITRC) recently announced its [2017 Data Breach report](#) and it's no surprise that breaches are up. Last year there were 1,579 data breaches exposing nearly 179 million records.

That represents a 44% increase in the number of breaches and a 389% increase in records exposed

The IRTC report stated that the number of credit card numbers exposed in 2017 totaled 14.2 million, up 88% over 2016. In addition, nearly 158 million [Social Security numbers](#) were exposed in 2017, an increase of more than eight times the number in 2016.



Dark Web Prices



Social Security
\$1



DDOS as a service
~\$7 per hour



Medical record
\$50 and up



Credit card data
\$0.25 to \$60



Bank account info
**\$1,000 and up
depending on the
account type and balance**



Mobile malware
\$150



Spam
**\$50 for ~500,000
emails**



Exploits
\$1,000-\$300,000



Maleware development
**\$2,500
(Commercial malware)**



Facebook account
**\$1 for an account
with 15 friends**

SOURCE: RSA

CNBC

THE CHANGING FACE OF **IDENTITY THEFT**

Examples of Personal Information

Information about you:

- Name
- Date of birth
- Social security number
- Address/Phone Number
- Driver's license
- Healthcare information
- Usernames and passwords

Information about your finances:

- Credit or debit card numbers
- Bank accounts numbers
- Investment account numbers
- Bank account log-in information

THE CHANGING FACE OF **IDENTITY THEFT**

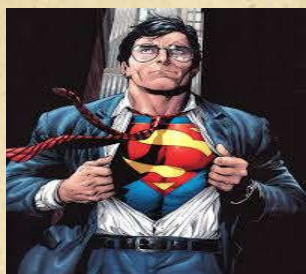
Types of Identity Theft

- **Synthetic**
- **Child**
- **Financial**
- **Medical**
- **Social Media**
- **Tax-related**
- **Criminal**
- **Deceased**

THE CHANGING FACE OF IDENTITY THEFT

Synthetic Identity

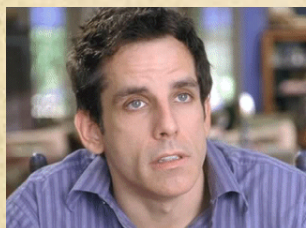
Sample Identities



Name: Clark Kent

DOB: 06/01/1983

SSN: xxx-xx-0001



Name: Gaylord Focker

DOB: 01/13/1972

SSN: xxx-xx-0002



Name: Clarice Starling

DOB: 10/9/1958

SSN: xxx-xx-0003

Sample Synthetic Identity



THE CHANGING FACE OF IDENTITY THEFT

Child Identity Theft

Why are children targets?

- A child's Social Security number likely to not be associated with an existing credit profile
- Theft has greater potential to go undetected for longer period of time
- Information can be easily accessible if perpetuated by family



THE CHANGING FACE OF IDENTITY THEFT

Financial Identity Theft

- Accounts for about **ONE-THIRD** of all identity theft cases
- Occurs when a thief obtains information about a victim with the intent of conducting fraudulent transactions
- Bad credit or financial status does **NOT** exclude you as a target

THE CHANGING FACE OF IDENTITY THEFT

Medical Identity Theft

When a thief uses your personal information (name, social security number, health insurance number, etc.) to:

- see a doctor
- get prescription drugs
- file claims with your insurance provider
- obtain medical equipment
- or get other care

How can thieves get your medical & personal information?

- Data breaches
 - This type of data is typically more valuable than credit card numbers (\$1-\$7) and can sometimes go for around \$50 on the black market
- Friends & Family
- Lost/stolen wallet, purse, etc.

THE CHANGING FACE OF IDENTITY THEFT

- Submit a report about the theft to the [Federal Trade Commission's website](#) or call the FTC's toll-free hotline at 1-877-IDTHEFT (438-4338).
- Consider placing a [freeze or fraud alert](#) on your credit reports.
- If you are the victim of medical ID theft, notify your insurer and medical providers, get copies of your medical files and ask to have them corrected. You can also consider filing a health-privacy complaint with [the U.S. Department of Health & Human Services online](#) or call 1-800-368-1019.

THE CHANGING FACE OF IDENTITY THEFT

Identity Theft Through Social Media

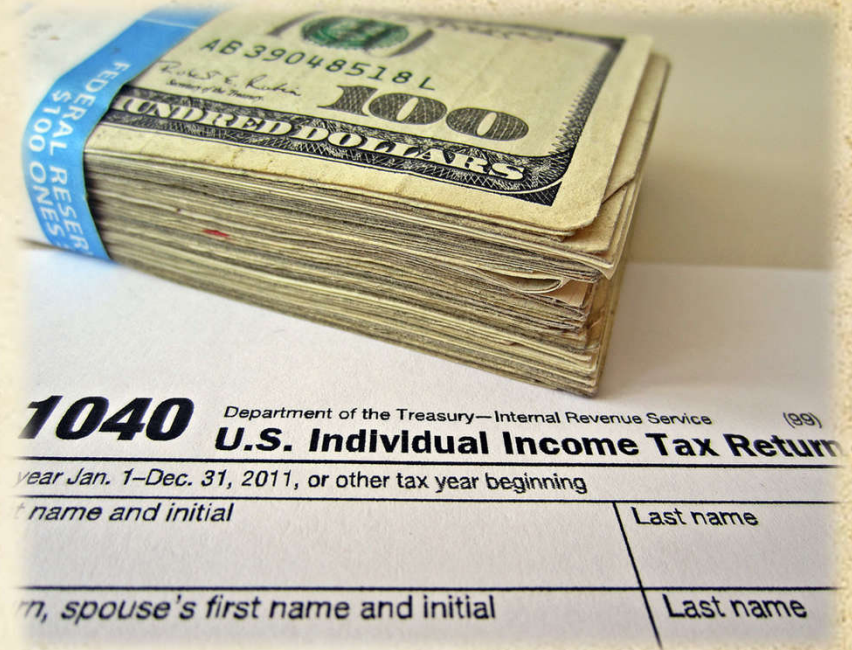
- Social Media profile elements can be used to steal or misappropriate your identity.
- Often social media is used to scam, slander, stalk, etc.
- Teens are most likely to 'over-share' on social media.
- In 2017, Facebook admitted that up to 270 million accounts are fake.



THE CHANGING FACE OF IDENTITY THEFT

Tax-related Identity Theft

- Occurs when someone uses your Social Security # to file a tax return claiming a fraudulent refund
- The IRS receives more than 1 million fraudulent returns each year
- In 2016, the IRS identified & confirmed 31,578 fraudulent tax returns, preventing the issuance of \$193.8 million in fraudulent tax refunds
- **HEADS UP!** New scam involves a fake IRS tax notice that claims you owe money as a result of the Affordable Care Act




LEGAL
RESOURCES

documents, such as corrected W-2, 1099, or missing forms that support your statement.

Note: You can fax documentation to [REDACTED]

2. Indicate your payment option

I am enclosing (check all that apply):

- ☐ Full payment of \$ [REDACTED]
- ☐ Partial payment of \$
- ☐ No payment
- ☐ A completed Installment Agreement Request (Form 9465)
 - Write your Social Security number [REDACTED] the tax year (2013), and the notice number (CP2000) on your payment and any correspondence.
 -  • Make your check or money order payable to the United States Treasury.

3. Authorization optional

If you would like to authorize someone, in addition to you, to contact the IRS concerning this notice, please include the person's information, your signature, and the date.

The authority granted is limited as indicated by the statement above the signature line. The contact may not sign returns, enter into agreements, or otherwise represent you before the IRS. If you want to have a designee with expanded authorization, see IRS Publication 947, Practice Before the IRS and Power of Attorney.

THE CHANGING FACE OF IDENTITY THEFT

Where are you Vulnerable?



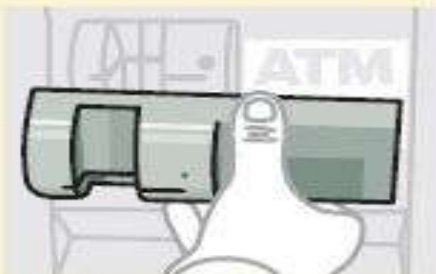
- Lost/Stolen mail, purse, or wallet
- Shoulder surfing
- Public Wi-Fi
- Corporate Breaches
- Social Media
- **Skimming**
- **Phishing**
- **Ransomware**

THE CHANGING FACE OF IDENTITY THEFT

Skimming

How debit-card/credit-card skimming works

Skimmers are electronic devices used to copy information from the magnetic strips on credit cards to create 'clone' credit cards or make Internet purchases. Thieves either use or sell the 'clone' cards.



ATMs

The device fits over the real ATM card-reader slot. ATM users do not know their information is being intercepted as their card is inserted into the false reader.



Gasoline pumps

The device is installed inside a gas pump in minutes and not visible to users. A gas-pump key can fit pumps in other stations.



Handheld

Someone can take your credit card and quickly record the information with a swipe on these small devices.



Keystroke logger

This device can be attached to a public-use computer, credit-card point-of-sale device or library computer and record passwords and other personal data.

THE CHANGING FACE OF IDENTITY THEFT

Phishing



My Netflix Profile

* Email Address:

* Email Password:

* Full Name:

* Billing Address:

* City:

* State:

* Zip Code:

* Billing Phone Number: (xxx-xxx-xxxx)

* Mother maiden name:

* Date of birth: / / (mm/dd/yyyy)

* Social Security Number:

* Bank Name:

* Card Number:    

* Expiration Date: - month - / - year -

* Card Verification Number:

* ATM Pin:

Update Credit Card

© 2011 Netflix, Inc.

Website

Watch Instantly
Browse DVDs
Your Queue
Movies You'll Love
How to watch on your TV

Membership

Your Account & Help
Gifts: Buy / Redeem
Tell-a-Friend

Company

About Us
Affiliates
Investor Relations
Media Center
Jobs
Contact Us
Blog

Community

Facebook Connect
Developers
App Gallery
Netflix Prize
RSS feeds
Friends



Member Sign In


Email

Password

☐ Remember me on this computer.

[What's this?](#)

Continue

 Secure Server

Not a member? [Click here.](#)

Need help signing in? [Click here.](#)

Terms of Use and Privacy Policy.
and U.S. Patent No. 6,584,450.

THE CHANGING FACE OF IDENTITY THEFT

What is Ransomware?

It is the generic term for **ANY MALICIOUS** software demanding ransom be paid by the device's user.

A typical method of infection would be to open an unsolicited email attachment or click on a link claiming to come from your bank or a delivery company.

THE CHANGING FACE OF IDENTITY THEFT

What is Ransomware?

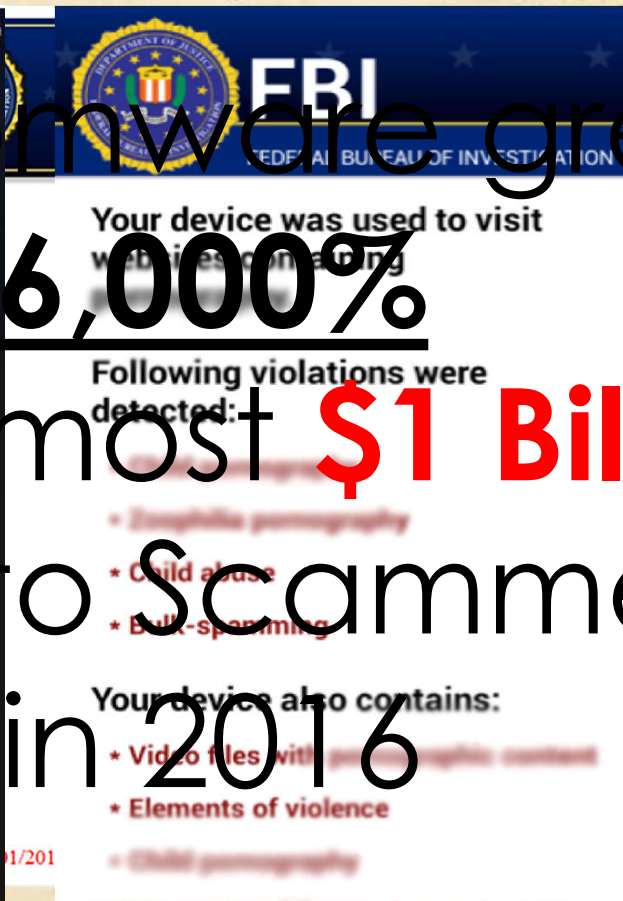
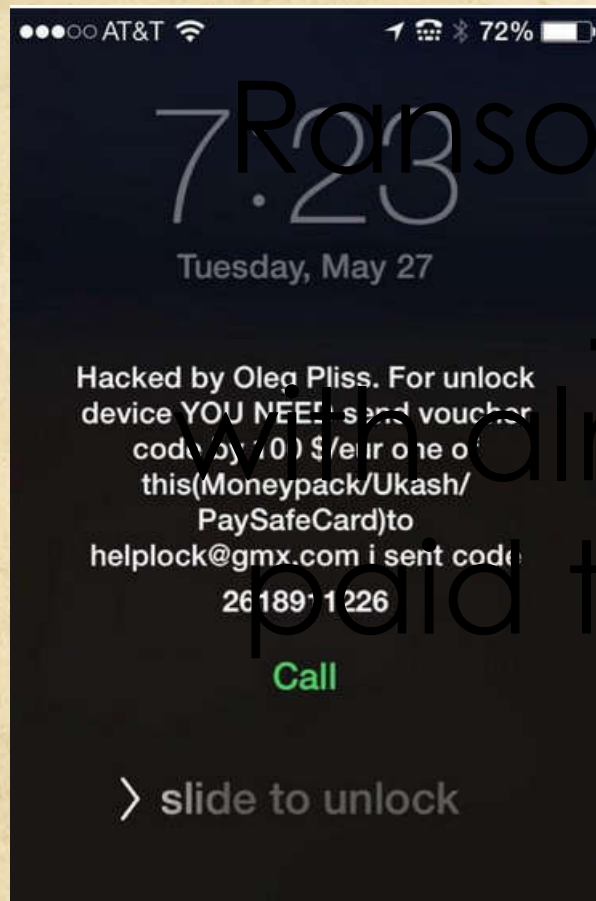
Why would you pay?

A virus has compromised your computer or data.

- Encrypted your documents or locks your device
- **THEN** demands you pay a ransom to unlock them
 - Ransom costs between \$200 and \$10,000 (FBI)

THE CHANGING FACE OF IDENTITY THEFT

What does Ransomware look like?



Ransomware grew by
6,000%
with almost \$1 Billion
paid to Scammers
in 2016

LEGAL
RESOURCES

THE CHANGING FACE OF **IDENTITY THEFT**

Ransomware Prevention and Recovery Tips

1. Regularly back-up your files
2. Employ proactive anti-virus software
3. Use web and email filtering

THE CHANGING FACE OF IDENTITY THEFT

Identifying Red Flags

- Unexplained transactions
- Debt collectors call about debts you aren't aware of
- Medical bills from services you did not receive
- Notification that your account information was compromised by a data breach
- Account Freezing



THE CHANGING FACE OF IDENTITY THEFT

Steps to Take if you are a Victim

- Contact one credit reporting agency to place a Fraud Alert and the other two will be notified
- Order free copies of your credit report
- File reports with the Federal Trade Commission and the police
- Contact creditors and close accounts that have been compromised
- Keep accurate records



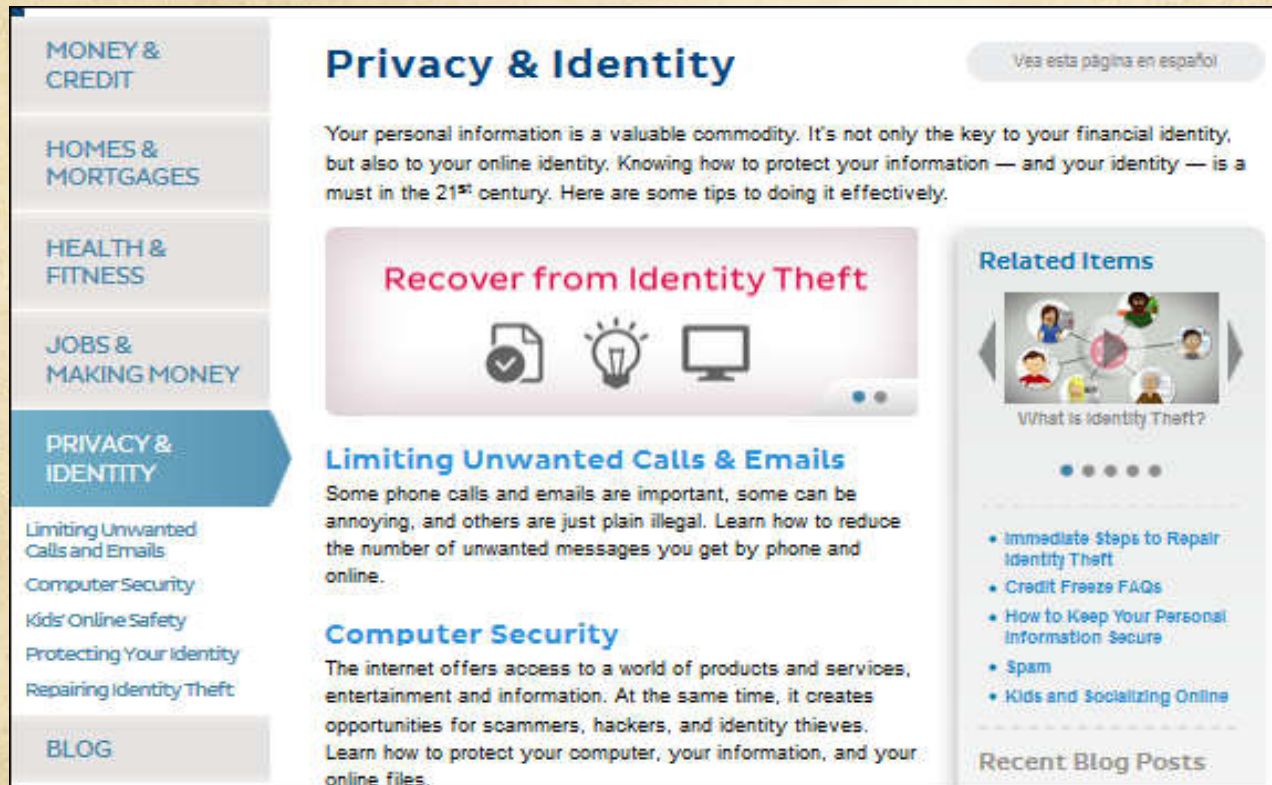
THE CHANGING FACE OF IDENTITY THEFT

Tips to Protect Yourself

- **Monitor** your credit reports - www.annualcreditreport.com
- **Review** all your financial/medical statements
- **Shred** or lock up personal information at home
- Use a **Password Manager** for all of your accounts
- Make sure your cell phone is wiped clean before disposing of it
- Secure your social media sites
- Enroll in an Identity Protection Plan with Insurance

THE CHANGING FACE OF IDENTITY THEFT

Federal Trade Commission (FTC)



The screenshot shows the FTC's "Privacy & Identity" webpage. On the left is a navigation menu with categories: MONEY & CREDIT, HOMES & MORTGAGES, HEALTH & FITNESS, JOBS & MAKING MONEY, and PRIVACY & IDENTITY (which is highlighted). Below the menu are links for "Limiting Unwanted Calls and Emails", "Computer Security", "Kids' Online Safety", "Protecting Your Identity", and "Repairing Identity Theft", followed by a "BLOG" link. The main content area is titled "Privacy & Identity" and includes a sub-header "Recover from Identity Theft" with icons of a document, a lightbulb, and a computer. Below this are sections for "Limiting Unwanted Calls & Emails" and "Computer Security". A "Related Items" sidebar on the right features a carousel titled "What is Identity Theft?" and a list of links: "Immediate Steps to Repair Identity Theft", "Credit Freeze FAQs", "How to Keep Your Personal Information Secure", "Spam", and "Kids and Socializing Online". At the bottom right of the sidebar is a "Recent Blog Posts" section. A link "Vea esta página en español" is visible in the top right of the page content.

MONEY & CREDIT

HOMES & MORTGAGES

HEALTH & FITNESS

JOBS & MAKING MONEY

PRIVACY & IDENTITY

Limiting Unwanted Calls and Emails

Computer Security

Kids' Online Safety

Protecting Your Identity

Repairing Identity Theft

BLOG

Privacy & Identity

Vea esta página en español

Your personal information is a valuable commodity. It's not only the key to your financial identity, but also to your online identity. Knowing how to protect your information — and your identity — is a must in the 21st century. Here are some tips to doing it effectively.

Recover from Identity Theft

Limiting Unwanted Calls & Emails

Some phone calls and emails are important, some can be annoying, and others are just plain illegal. Learn how to reduce the number of unwanted messages you get by phone and online.

Computer Security

The internet offers access to a world of products and services, entertainment and information. At the same time, it creates opportunities for scammers, hackers, and identity thieves. Learn how to protect your computer, your information, and your online files.

Related Items

What is Identity Theft?

- Immediate Steps to Repair Identity Theft
- Credit Freeze FAQs
- How to Keep Your Personal Information Secure
- Spam
- Kids and Socializing Online

Recent Blog Posts

<http://www.consumer.ftc.gov/topics/privacy-identity>

LEGAL[®]
RESOURCES

THE CHANGING FACE OF IDENTITY THEFT

Victims:

- Close accounts that have been affected
- File a report with the Federal Trade Commission
IdentityTheft.gov or call 1-877-ID-THEFT (438-4338)
The FTC will provide you with a recovery plan
- File a police report
Keep a copy of the report to send to creditors
- Place a fraud alert on your credit reports and review them frequently
Equifax: 1-800-525-6285 | www.equifax.com
Experian: 1-888-397-3742 | www.experian.com
TransUnion: 1-800-680-7289 | www.transunion.com
- Change all account passwords

THE CHANGING FACE OF IDENTITY THEFT

Credit Freeze

- A state right
- Minimal *fee **\$10 for each bureau** for VA residents (varies by state)
- May apply for credit using a PIN to lift the freeze temporarily
- Must notify each credit agency separately
- Creditors **CANNOT** view credit report

Extra Level of Protection

Fraud Alert

- A federal right for possible and actual victims
 - **FREE**
- Lasts *90 days; renewable
- Red flag for new creditors
- One credit agency must notify other two
- 3 types (90 day, Extended, Active Duty Military)
- Creditors can view credit report

* **September 2018:** Credit Freeze are *FREE*.
Fraud Alerts will extend to *1 year*.

THE CHANGING FACE OF IDENTITY THEFT

- Phishing = Fraudulent Emails
- Pharming = Directed to fake websites
- Vishing = Telephone scams
- Smishing = Fraudulent text messages

What Should You Do?

- ✓ Review emails carefully; look at sender's address and links; look for typos; don't open attachments if in doubt.
- ✓ Don't click on links and log in to accounts; go independently from your browser.
- ✓ Use encryption software to keep malware from seeing your keyboard.
- ✓ Look if a website uses https; s for security.
- ✓ Block robocalls with services like Nomorobo.com.
- ✓ Don't respond to unrecognized text numbers.

- **Donate to charities you know and trust** with a proven track record with dealing with disasters.
- **Be alert for charities that seem to have sprung up overnight in connection with current events.** Check out the charity with the [Better Business Bureau's \(BBB\) Wise Giving Alliance](#), [Charity Navigator](#), [Charity Watch](#), or [GuideStar](#).
- **Designate the disaster** so you can ensure your funds are going to disaster relief, rather than a general fund.
- **Never click on links or open attachments in e-mails unless you know who sent it.** You could unknowingly install [malware](#) on your computer.
- **Don't assume that charity messages posted on social media are legitimate.** Research the organization yourself.
- **When texting to donate, confirm the number with the source before you donate.** The charge will show up on your mobile phone bill, but donations are not immediate.
- **Find out if the charity or fundraiser must be registered in your state** by contacting the [National Association of State Charity Officials](#). If they should be registered, but they're not, consider donating through another charity.



THE CHANGING FACE OF IDENTITY THEFT

To Learn More...

- Visit us at www.LegalResources.com
- Social Media:



@legal_resources



legalresources

LEGAL[®]
RESOURCES

THE CHANGING FACE OF **IDENTITY THEFT**

Don't let imposters get too close...



LEGAL[®]
RESOURCES