Identity Theft - An Ongoing Problem

Identity theft is one of the most widespread crimes in the world. And while awareness of this crime has grown over the years, it continues to be a prevalent problem. Also known as identity fraud, this practice involves wrongfully obtaining and using another individual's personal data for illicit financial gain or other types of fraud. Thieves use Social Security numbers, credit card numbers, and personal information, like usernames and passwords, to buy cars, open new credit accounts, or forge identification cards.

There are five types of identity theft: criminal, financial, medical, child, and identity cloning. Criminal identity theft happens when an individual poses as another when apprehended for a crime. Financial and medical identity theft involve using another's identity or personal information to obtain goods, services, medical care, or drugs. Child identity theft occurs when a thief uses a minor's Social Security number. And in identity cloning, a thief will impersonate someone else to conceal his or her true identity.

Terms to Know

- Data breach – The unintended release of information, compromising the security of personal information.
- Shoulder surfing – Watching or listening while another individual provides credit card or other personal information.
- Skimming – Copying a credit card's magnetic strip in order to obtain the credit card numbers.
- Phishing – Sending emails that direct recipients to fake, but legitimate-looking, websites that ask for personal information.
- Pharming – A method wherein thieves redirect a website's traffic to a fake site.

Identity Theft Statistics:

- On average, there are over 11 million victims of identity fraud each year.
- There is one victim of identity fraud every three seconds.
- Identity thieves steal about $20 billion each year.
- 25% of consumers involved in data breaches become victims of identity fraud.
- It takes about a month and a half before the fraud is discovered.
- 18- to 29-year-olds are the most frequent victims.

RESOURCES

Identity Theft Resource Center

www.idtheftcenter.org/Protect-yourself/id-theft-prevention-tips.html

National Crime Prevention Council

www.ncpc.org/cms-upload/prevent/files/IDtheftrev.pdf

The United States Department of Justice

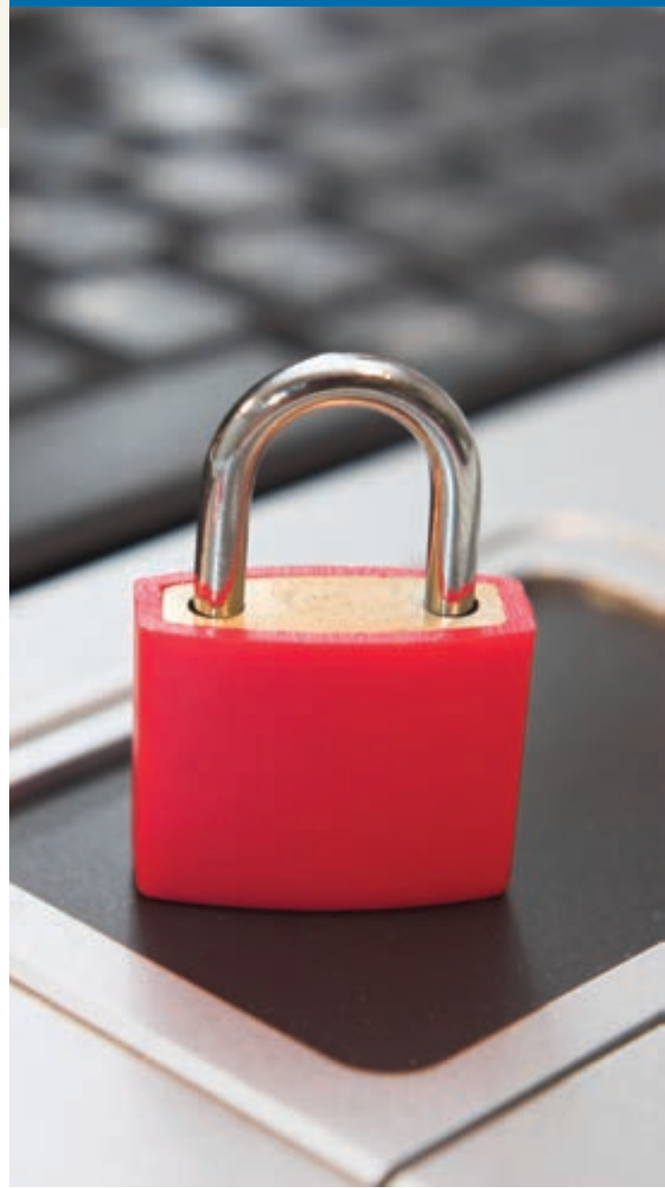
www.justice.gov/criminal/fraud/websites/idtheft.html

GET YOUR LIFE >INFOCUS

P.O. Box 6986 Metairie, LA 70009-6986 • 877-329-0578
www.ESPublish.com • product #PB-PS156

>INFOCUS

PREVENTING IDENTITY THEFT



Common Identity Theft Methods

Thieves have a variety of ways to get your personal information, many of which involve physically stealing from you. They may steal:

- Credit card payments from private mailboxes.
- Your mail, especially credit card applications.
- Wallets and purses.
- Social Security cards.

Identity thieves can also:

- File a change of address in your name to obtain personal and financial information.
- Dig through your garbage looking for financial statements, pre-approved credit card offers, or canceled checks.
- Lift information from checks, medical charts, or driver's licenses.
- Pretend to be business people who are gathering personal information.
- Photograph credit or debit cards while you're making purchases or using an ATM.
- Hack into your computer to steal your personal information.

Identity Theft Prevention

Being proactive is the most crucial element of preventing identity theft!

With Personal Finances:

- Check your credit reports at least once a year. You'll want to pay attention to all open and closed accounts as well as negative items to ensure they match up with your records. Also, look into all credit inquiries that have been made. Unusual inquiries may indicate that thieves are trying to fraudulently open accounts.
- Examine your bank and credit card statements regularly, and watch out for errors or unfamiliar charges.
- Shred financial statements, pre-approved credit card offers, canceled checks, and other sensitive documents before throwing them out.
- Know your billing cycles. If a bill fails to show up, call to find out why.
- Pick up new checks at the bank instead of having them mailed to you.
- Don't write down your account number on the outside of bill payment envelopes.
- If possible, pay bills online using a secure site and only give your credit card number online when it is encrypted on a secure site.
- Keep your financial records inside a locked filing cabinet or safe.

At Home:

- Don't write down your passwords – commit them to memory.
- On old computers, destroy the hard drive before selling it or giving it to charity.
- Instead of depositing outgoing mail in a personal curbside mailbox, use a United States Postal Service mailbox or take it directly to the post office.
- Don't give out personal or financial information over the phone or Internet.
- Be wary of people calling who claim to be bank or government employees. Don't provide any personal information. Call the bank directly and inform them of the situation.

Out and About:

- Carry as few credit and identification cards as possible. And don't carry your Social Security card with you!
- Be aware of people watching you while you're using an ATM machine or purchasing something with a debit card. Shield the screen so thieves cannot see your password.

Always treat your Social Security number as confidential information. Provide it only when necessary. Government organizations, including the Internal Revenue Service, Department of Education, Veterans Administration, the U.S Treasury, and Medicaid, require that you provide your Social Security number. Banks and employers will also need your number.

You may be asked for this number when applying for credit cards, opening utility company accounts, or getting a cell phone. These types of companies will use your Social Security number to check your credit. And in some cases, there are alternative routes available if you don't feel comfortable providing this information.

If You've Been a Victim

Even if you've been proactive and vigilant, there's still a risk for identity theft. While you may be guarding your personal information, it doesn't mean that other individuals and companies are just as watchful. Should you discover that your personal information has been compromised:

- Contact the credit reporting agencies and have them flag your account.
- Notify your creditors about unauthorized charges.
- Check your bank accounts and close them if necessary.
- Contact the police and file a report about the identity theft. You'll need the police report for creditors. If the crime took place in a different area, you'll have to contact the police in that area as well.
- You may also need to contact the Social Security Administration, Internal Revenue Service, Federal Trade Commission, and the U.S. Postal Inspection Service, depending on the type of fraud.