9-1-1

City of Roseville Public Safety | Police

February 2017

Identity Theft

What is identity theft?

You've probably heard the news story of a data breach where clients' Social Security numbers and other personal information were hacked by criminals. Perhaps you have even received a letter from your insurance company or financial institution letting you know that your personal information was comprised. If so, you could be the victim of identity theft.

According to the U.S. Department of Justice, identity theft (or fraud) is a term used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

How do criminals obtain your personal information?

Criminals can easily obtain your personal data without having to break into your home. Here are just a few examples:

- "Shoulder surfing"—someone watches from a nearby location or over your shoulder as you punch in your credit card/ATM number.
- Someone listens in on a conversation as you give your credit card number to a hotel or rental car company.
- Someone looks through your mail for "pre-approved" credit card letters.
- Data breaches.

Everyone is susceptible to ID theft. However, there are things you can do to reduce your risk of becoming a victim.

Top tips for identity theft protection

How to prevent ID theft.

The State of California, Office of the Attorney General, offers the following tips for ID theft protection:

- **Protect your Social Security number.** Don't carry your card with you.
- **Fight "phishing" - don't take the bait.** Scam artists "phish" for victims by pretending to be banks, stores, or government agencies. They do this over the phone, in email, and in regular mail. Don't respond to any request to verify your account number or password.
- **Polish your password practices**. Use different passwords for all your accounts. Passwords should be at least eight characters, with a mix of letters, numbers and symbols.
- **Be mysterious on social networks.** Don't share your home or email address, children's names, birthdate, etc. Thieves can use them for scams, phishing, and account theft.
- **Shield your computer and smartphone**. Use firewall, virus and spyware protection software you update regularly.
- **Check your statements**. Open your credit cards bills and bank statements right away. Check them carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time.
- **Stop pre-approved credit offers.** Call 1-888-5OPTOUT or go online at www.optoutprescreen.com.
- **Check your credit reports for free.** Call 1-877-322-8228 or online at www.annualcreditreport.com

Warnings signs of identity theft

What do thieves do with your information?

Once the thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. Additionally, they can file a tax return in your name.

Clues that someone has stolen your information.

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.

Source: idtheft.gov

Report identity theft

If you are a victim of identity theft, you can file an online report with the Roseville Police Department at www.roseville.ca.us/police (Select the "Submit a Report On-line" button on the right hand side of the screen) or call 774-5000 (option 1).

Also visit the Federal Trade Commission's website (identitytheft.gov) to report and recover from identity theft.

Follow us on social media:

ROSEVILLE PUBLIC SAFETY

9-1-1 City of Roseville Public Safety | Police February 2017

Top Ten Scams

Better Business Bureau's top scams of 2016

The Council of Better Business Bureaus has released the Top Ten Scams of 2016. Tax scams still remain number one on the list despite the police raid in Mumbai, India. In 2015 Tax Scams accounted for 24 percent, and in 2016 they accounted for 25 percent of scams reported.

This list was compiled based on more than 30,000 scams reported to BBB Scam Tracker, a free interactive tool launched last year by the BBB Institute for Marketplace Trust.

The top three scams on the 2016 list – tax scams, debt collection scams, and sweepstakes/prizes/gifts scams – were the same as in 2015. New to the top ten are online purchase scams (#4) and phishing scams (#10). Online purchase scams were common in 2015 as well, but this scam type was not added as a BBB Scam Tracker category until 2016. Employment scams (#5) are also new to the top ten, but only because work-from-home scams, previously a separate category, were included. Another change was the drop of tech support scams from #4 last year to #7 this year.

2016 Top Scams

1. **Tax Scams-**Someone calls and claims to be with the IRS and says that you owe money. Unless you pay immediately you will be arrested. Note: The IRS will not call. They will send a certified letter.
2. **Debt Collections-**Someone calls and claims you have an unpaid debt. You are threatened with garnishment, lawsuit, or jail time if you don't pay right away.
3. **Sweepstakes/Prizes/Gifts**-You receive a letter, phone call, or email claiming you have won a prize in a sweepstake. However, you have to send a fee to claim the prize.
4. **Online Purchase**-You make a purchase but never receive the item. Scammers set up fake sites in order to steal your money or personal/ financial information.
5. **Employment**-You answer an online ad for a job offer. In order to get the job, you have to pay a fee.
6. **Government Grant**-You receive a phone call, email, or letter informing you that you've qualified for a government grant. In order to receive the grant you have to pay a fee.
7. **Tech Support**-You are contacted by a "tech" claiming to have detected a virus on your computer. To remove the virus, the tech needs to take control of your computer. Letting someone access your computer allows him/her to steal personal information or install malware.
8. **Advance Fee Loan**-You fill out an application online for a loan and soon receive an email or phone call advising you are approved for the loan but must pay a fee. You pay but never see the loan.
9. **Fake check/Money Order**-Someone pays you for goods or services. You receive a check in the mail that is larger than the amount owed. You are asked to deposit the check and send back the difference. The fake check bounces and you are out the money.
10. **Phishing**-You receive an email telling you that you've won a contest or a company needs to verify your personal information. This is known as "phishing." Links or attachments in the email can allow malware to be downloaded onto your computer.

Source: BBB

Report fraud

Where to file complaints:

According to AARP (American Association of Retired People) the most frequent Google search related to scams is "How do I report a scam?" Wondering where to report a scam? Here's a list compiled by AARP.

Federal Trade Commission (ftc.gov/complaint or 877-382-4357) This is the agency for reporting identity theft, abusive debt collectors and most types of fraud.

National Do Not Call Registry (donotcall.gov or 888-382-1222) For reporting unsolicited sales calls.

Consumer Financial Protection Bureau (consumerfinance.gov/complaint or 855-411-2372) To report complaints with a financial product or service.

Internet Crime Complaint Center (ic3.gov/complaint) For reporting internet-based scams, including online auctions; investment and sales fraud; internet extortion, hacking and phishing; and scam emails. This site is operated by the FBI.

Postal Inspection Service (postalinspectors.uspis.gov or 877-876-2455) To report scams distributed by U.S. mail, such as bogus lottery and sweepstakes "winnings," chain-letter schemes and deceptive advertisements—as well a mail theft.

Sources: *AARP, Better Business Bureau, Federal Trade Commission, idtheft.gov*

Police Department
1051 Junction Blvd.
Roseville CA 95678
(916) 774-5000
www.roseville.ca.us/police

Call 9-1-1
EMERGENCY
IN PROGRESS

Abandoned Vehicle Hotline
(916) 746-1022

Alarms/Alarm Permits
(916) 774-5093

Animal Control
(916)774-5090

Community Events & Neighborhood Watch
(916) 774-5050
PDCommunityServices@roseville.ca.us

Graffiti Abatement
(916) 746-1021

Police News & Crime Alert Emails:
www.roseville.ca.us/enotify

RCONA
(Roseville Coalition Of Neighborhood Associations)
www.RCONA.org

The "9-1-1" is published for City of Roseville's residents by the Community Relations Division of the Roseville Police Department. Please send comments or suggestions to pdcommunityservices@roseville.ca.us, (916) 774-5050.
Vol. 17 Issue 02