

Identity Theft

Identity theft can happen to anyone. It is a serious crime that can disrupt your finances, credit history, and reputation. Identity theft happens when someone steals your personal information and uses it without your permission.



According to the Federal Trade Commission identity thieves might:

- go through trash and dumpsters stealing bills and documents that have sensitive information.
- work for a business, medical office, or government agency and steal personal information on the job.
- misuse the name of a legitimate business and trick you into revealing personal information.
- Pretend to offer a job, loan, or an apartment and ask you to send personal information to “qualify.”

- Steal your wallet, purse, backpack, or mail and remove your credit cards, driver’s license, insurance card, and other items that show personal information.

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new accounts, or get medical treatment on your health insurance. An identity thief might even file a tax return in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

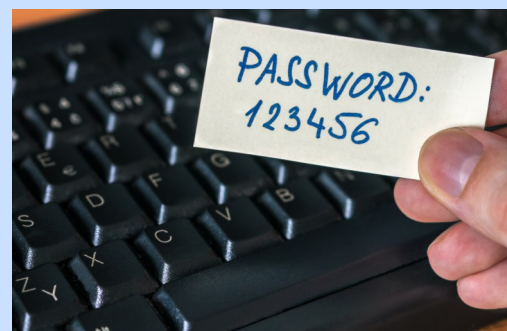
Is Your Password Secure?

Splash Data has revealed their annual list of America’s “worst passwords” and, therefore, most easily guessed by hackers. If your password is amongst those listed, you should consider changing it immediately.

- #1 123456
- #2 password
- #3 12345678
- #4 qwerty
- #5 12345
- #6 123456789
- #7 football

- #8 1234
- #9 1234567
- #10 baseball
- #11 welcome
- #12 1234567890
- #13 abc123
- #14 111111
- #15 1qaz2wsx
- #16 dragon
- #17 master
- #18 monkey
- #19 letmein
- #20 login

- #21 princess
- #22 qwertyuiop
- #23 solo
- #24 passw0rd
- #25 starwars



Red Flags of ID Theft



Here are some “red flags” on identity theft from the Federal Trade Commission.

- Mistakes appear on your bank, credit card, or other account statements.
- Mistakes on the “explanation of medical benefits” from your health plan appear.
- Your regular bills and account statements don’t arrive on time.
- You receive bills or collection notices for products or services you never received.
- Unwarranted collection notices on your credit report are found.
- Businesses turn down your checks.
- You are turned down unexpectedly for a loan or job.
- The IRS notifies you that someone else used your social security number to file a tax return.

FTC Announces Significant Enhancements to IdentityTheft.gov

One-Stop Website Offers Array of New Tools for ID Theft Victims; Free Recovery Plans Will Assist Consumers in Alerting Police, Credit Agencies, IRS

For the first time, identity theft victims can now go online and get a free, personalized identity theft recovery plan as a result of significant enhancements to the Federal Trade Commission’s IdentityTheft.gov website.

The new one-stop website is integrated with the FTC’s consumer complaint system, allowing consumers who are victims of identity theft to rapidly file a complaint with the FTC and then get a personalized guide to recovery that helps streamline many of the steps involved.

Follow us on social media:



How to Protect Your Information

The Federal Trade Commission offers the following tips on how to protect your personal information.

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Go to annualcreditreport.com or call 1-877-322-8228.
- Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a

statement has mistakes, contact the business.

- Shred all documents that show personal, financial, and medical information before you throw them away.
- Don't respond to email, text, and phone messages that ask for personal information. Legitimate companies don't ask for information this way. Delete the messages.
- Create passwords that mix letters, numbers, and special characters.

Don't use the same password for more than one account.

- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure.
- Set your computer's operating system web browser, and security system to update automatically.
- If you use a public wireless network, don't send information to any website that isn't fully encrypted.



IRS Scam

Last year the IRS scam was a big one, and this year appears to be no exception. According to Consumer Reports scammers impersonated the IRS and intimidated consumers into paying penalties for "back taxes." This scam accounted for nearly a quarter of all scams reported to the Better Business Bureau in 2015. The

scammers often used phone spoofing, which made the number they called from show up as "IRS" on the caller ID.

Tip

The IRS will never call you and demand immediate payment, ask for credit or debit card numbers over the phone, or threaten you with imprisonment. The IRS only contacts people via U.S. mail.

What is a Credit Freeze?

Are you concerned about ID theft, a mega-data breach, or someone gaining access to your credit report without permission? You may want to consider placing a credit freeze on your report.

A credit freeze, or security freeze, allows you to restrict access to your credit report. This makes it more difficult for ID thieves to open new accounts in your name. Creditors need to see your credit report before they approve a new

account. If they can't see your file, they most likely will not extend credit.

To freeze your credit reports contact each of the three credit reporting bureaus or complete the freeze on each company's website.

A security freeze is free to ID theft victims who have a police report of ID theft. Otherwise if you are under 65 years of age it will cost you \$10 for each of the three credit bureaus or \$5 each if you are over 65.



Credit Reporting Bureaus

Equifax:

www.equifax.com
Phone: 1-800-525-6285
Mail: Equifax Information Service
P.O. Box 740256
Atlanta, GA 30348

Experian:

www.experian.com
Phone: 1-888-397-3742
Mail: Experian
P.O. Box 4500
Allen, TX 75013

TransUnion:

Transunion.com
Phone: 1-800-680-7289
Mail: TransUnion
P.O. Box 105281
Atlanta, GA 30348-5281

Sources: Federal Trade Commission (FTC), Splash Data, Consumer Reports

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. 16 Issue 02