Debt.com®

When life happens...

Protect Against Identity Theft

Keeping personal information safe & what to do if it happens to you

An Identity Theft Epidemic

Identity theft is a huge business in the U.S. and around the world. As the world changes and more financial transactions are moved online and into a digital world, it's becoming more and more risky each year. So much so that last year an identity theft case effectively occurred every one minute three seconds in this country.

Statistics show 85% of all identity theft victims find out about the theft in a negative way, such as being denied for credit because of a bad credit check. This can be costly and frustrating. You can be denied on a mortgage or car loan which could delay vital financial moves that you need to make. What's more direct cash losses on identity theft totaled over $221 billion in the last year alone.

When Life Happens...

With so much potential time and money wasted on addressing an identity theft problem, not to mention the hassle and stress it will cause in your life, there's plenty of good reason to take steps to protect your identity. If you get into trouble with identity theft or would like more information about identity theft prevention, visit our website www.Debt.com or call 800-810-0989 to get the answers you need.

Protect Your Identity the Digital World

The increasing popularity of online banking and shopping, paid online community accounts, and social networking has made the digital world the riskiest place for personal information. It's becoming almost impossible to avoid having at least some personal information online or using online marketplaces to shop, make travel reservations and more. Since you can't avoid it, your only option is to take every step possible to protect identity as much as possible.

The following tips can help you protect your identity online:

- **Never enter sensitive information on an unsecured website.** On a secured website, the address bar at the top of your browser will be green and the address will start with "https://" instead of just "http://".

- **For passwords on protected accounts, make every password unique and don't use things that others could easily guess.** Use combinations of capped and uncapped letters as well as numbers - something you can remember but others wouldn't be able to guess. Don't use the exact same password on every account.

- **Only shop on reputable websites.** Keep your shopping to reputable sites you know and/or look for trust seals, such as the TRUSTee and VeraSign logos to verify that the site is legitimate.

- **Avoid accessing accounts on a mobile hotspot or shared network.** Don't get into your personal accounts except on your own private network. This includes avoiding your accounts while you're on a network at your job or at school.

- **Close/cancel accounts that you don't use.** Never allow old accounts to remain online if you've cancelled a service. Check a company's privacy policy to determine how long your personal information will be kept on file once an account is closed.

- **Opt-out of allowing companies to share your personal information.** When you sign up for services, always make sure to opt-out of permitting the company to share the information you provide.

- **For peer-to-peer shopping websites, make sure a seller is legitimate before you make a purchase.** Online marketplaces like eBay allow you to review a seller's information and seller history before you buy, so you know a certain seller isn't a scam artist.

• **Don't use your debit card or a high-limit credit card for online shopping.** If your information is compromised, you don't want a thief to have access to your main bank account or a large credit line. If possible, use a prepaid credit card with a limited amount of money on it for online purchases.

• **Adjust the security settings on any social media accounts you use so that you don't share everything with everyone.** Any social site will allow you to adjust your settings so people you don't know can't see what you're posting. In addition, make sure not to share anything that's sensitive online - even with your friends.

• **Don't give out your login credentials.** This is like giving out the PIN number for your debit card - it's just not something you want to do even with someone you're really close to.

• **Never send sensitive information via email.** Even if it seems like the email request is legitimate and from a service provider you use, do not send bank account information, your social security number, etc. via email.

• **Only open email from people you know.** Otherwise, you may download a virus or install malware on your computer that can be used to access your information.

Protect Your Identity in the Physical World

Although online identity theft is the bigger news these days, traditional identity theft still happens. Whether you leave a credit card at a restaurant or let it out of your sight at a department store, your identity can still be at risk from traditional theft outlets.

The following tips can help you avoid identity theft issues while you're out:

• **Limit the cards you keep in your wallet to what you need to use.** Keeping rarely-used credit cards and specialty store cards in your wallet only gives thieves more opportunity.

• **Keep your wallet safe.** Don't leave your wallet in an unzipped purse or a pocket where it can be pulled out without noticing.

• **Don't let your credit card out of your sight.** Never allow a store attendant to take your credit card where you can't see it.

• **Cut up old credit cards and bank cards before you throw them away.** You don't want someone to fish your identity out of the garbage.

• **If possible, get a locking mailbox so bills and account statements can't be taken from your mailbox.** Your mail can contain sensitive personal and account information that can be used to steal your identity.

• **Buy an inexpensive shredder for your home.** This allows you to shred any documents or statements that contain your account information before they go into the trash.

• **Don't give out your social security number unless it's absolutely necessary.** Many businesses will request your SS# as part of the personal information they require on forms; you can ask if this field can be left blank.

• **Never give your PIN number to anyone.** Things change, relationships break apart and the last thing you need on top of a bad breakup is identity theft.

• **Don't use an ATM if you don't recognize the financial institution.** There are ways thieves can use a machine to obtain your personal information.

Making Sure Your Identity is Safe

Even with all of these protections, it's impossible to guarantee your identity will be safe. Corporate-wide data breaches, outright physical theft and many other issues can still put your identity at risk of theft even if you take every step possible to be careful. With that in mind, it's important to take regular measures to make sure your identity and personal information haven't been compromised.

The following tips can help you monitor your identity:

- **Check your credit report at least once each year.** Review your report to make sure you don't have any new accounts t hat you didn't open or lines of credit you didn't apply for.

- **Review Social Security benefit statements every year.** You can check the statement for errors and possible indications of fraud.

- **Use a credit monitoring service to stay updated on your account activity.** The added peace of mind for identity theft prevention is often worth the cost.

What to Do When Identity Theft Occurs

Don't wait around or procrastinate for any reason once you know that your identity has been stolen. Even if you're out of the country on vacation, take every step possible to ensure you can take steps to protect your accounts and your livelihood.

1. **File a police report.** You are likely to need documentation for any steps that follow and a police report is the right record to have when a crime has been committed.

2. **Notify the credit bureaus and ask that a fraud alert be placed on your file.** This prevents new accounts from being opened or credit checks to be run without your express permission.

3. **Fill out a fraud affifavit through the FTC.** This standard form is available through the FTC website at www.ftc.gov.

4. **Contact account issuers to cancel those accounts.** You should do this for any account you think has been compromised.

5. **Place a fraud alert on your driver's license.** This step only applies if your driver's license has been stolen or your DL# has been compromised.

6. **Check with the postal inspector to make sure a change of address hasn't been issued.** In some cases a savvy thief will forward your mail to a new address.

7. **Contact the Social Security Administration.** If you think your social security number has been compromised, then you need to contact the SSA office immediately.

8. **Alert the passport office.** This helps ensure a thief isn't issuing a new passport with your information.

9. **Review your credit report.** This way you can see how many accounts have been affected and if you need to take additional action to close your other accounts.

10. **Talk to an attorney early.** If you plan on filing a lawsuit, there is a two-year statute of limitations on fraud cases. You must file any claims as early as possible if you want to take legal action.

Notes

About Debt.com

At Debt.com we're dedicated to helping you handle whatever life brings your way when it comes to money. We understand that being 100% debt-free isn't realistic for most people, so we have develop strategies to help manage debt. With the right plan, debt can be an effective part of your financial outlook and help you reach your goals - whatever those goals might be.

If you're struggling with debt and don't know where to turn, we can help. We have solutions to address most debt and credit issues. That's why we say, **"When Life Happens...Debt.com."**

Visit **www.Debt.com** to find solutions or call **800-810-0989** to find the help you need.


created
MR