



# Identity theft

---

Deputy Les Wiemers  
Weld County Sheriffs Office  
Aims School Resource Officer



# Introduction

---

In the course of a busy day, you may:

- write a check
- charge tickets to a ball game
- rent a car
- mail your tax returns
- change service providers for your cell phone
- apply for a credit card.



# Cont...

---

- In each transaction, you reveal bits of personal information, like:
  - your bank and credit card account numbers
  - your income
  - your SSN
  - your name, address, and phone numbers.



# Cont...

---

Once a thief has that information, it can be used without your knowledge to commit fraud or theft.

# How identity theft occurs

## They may:

---



- steal your wallet or purse.
- steal your personal information through email or the phone by saying they're from a legitimate company and claiming that you have a problem with your account. This practice is known as "phishing".
- steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach a device to an ATM machine where they may enter or swipe your card.



## Cont...They may:

---

- get your credit reports by abusing the authorized access that was granted to their employer, or by posing as a landlord, employer, or someone else who may have a legal right to your report.
- rummage through your trash, the trash of businesses, or public trash dumps in a practice known as “**dumpster diving.**”



## Cont...They may:

---

- steal personal information they find in your home.
- steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.
- complete a “change of address form” to divert your mail to another location.

# What do ID thieves do with your name?

---



- They may call your credit card issuer to change the billing address on your account. The imposter then runs up charges on your account. Because the bills are being sent to a different address, it may be some time before you realize there's a problem.
- They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.



# Cont...

---

- They may establish phone or wireless service in your name.
- They may open a bank account in your name and write bad checks on the account.
- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.



# Cont...

---

- They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- They may buy a car by taking out an auto loan in your name.
- They may get identification such as a driver's license issued with their picture, in your name.



# Cont...

---

- They may get a job or file fraudulent tax returns in your name.
- They may give your name to the police during an arrest. If they don't show up for the court date, a warrant for arrest is issued in your name.

# How can you tell if you're a victim of Identity theft?

---



- If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report.
- You can find out by ordering a copy of your credit report from the three nationwide consumer reporting companies.



## Cont...

---

If you have lost any personal information – or if it has been stolen – you may want to check all your reports more frequently for the first year.

Remember to:

- Monitor the balances of your financial accounts.
- Look for unexplained charges or withdrawals.



## Other indications of identity theft can be:

---

- failing to receive bills or other mail. This could mean an identity thief has submitted a change of address.
- receiving credit cards for which you did not apply.
- denial of credit for no apparent reason.
- receiving calls from debt collectors or companies about merchandise or services you didn't buy.

# 4 immediate steps to take if you are victimized.

---



1. Place a fraud alert on your credit reports, and review your credit reports.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.
3. File a report with your local police or the police in the community where the identity theft took place.



# Cont...

---

## 4. File a complaint with the Federal Trade Commission

You can do so by logging on to:

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

Or you can call:

**(877) IDTHEFT**



# Free annual credit reports

---

An amendment to the Fair Credit Reporting Act **requires** each of the major nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months.



# Cont...

---

- To order your free annual report from one or all the national consumer reporting companies, visit:  
[www.annualcreditreport.com](http://www.annualcreditreport.com)  
**1-877-322-8228**
- Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through the above web site or phone number.



# Consider your computer

---

Your computer can be a goldmine of personal information to an identity thief. Here are some ways to help you keep your computer, and the personal information it stores, safe:

- Update your virus protection software regularly. Ideally, you should set your virus protection software to update automatically.



# Cont...

---

- Do not open files sent to you by strangers, click on hyperlinks, or download programs from people or companies you don't know. Be cautious about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.



## Cont...

---

- Use a firewall program, especially if you use a high speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program allows you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.



# Cont...

---

- If you need to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for secure).



# Cont...

---

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use what experts call a “strong” password – a combination of letters (upper and lower case), numbers, and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers. For example:

- “I love Felix; he’s a good cat,” would become 1LFHa6c.

Don’t use an automatic log-in feature that saves your user name and password, and always log off when you’re finished. If your laptop is stolen, it makes it harder for a thief to access your personal information.



# Cont...

---

- Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a “**wipe**” utility program to overwrite the entire hard drive.



## Cont...

---

- Look for website privacy policies, and read them. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy – or if you can't understand it – consider doing business elsewhere.



# Everyday diligence

---

- Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with.
- Treat your mail and trash carefully. Shred anything with your personal info on it.



# Cont...

---

- Don't carry your SSN card in your wallet; store it in a secure place.
- Carry only the identification information and the credit and debit cards that you'll actually need when you go out.



# Deputy Les Wiemers

If I can be of any help  
please let me know.

- Weld County Sheriffs Office
- Aims School Resource Officer
- Office: 970-356-4015 X4174
- Cell: 970-539-2171
- Email: [lwiemers@co.weld.co.us](mailto:lwiemers@co.weld.co.us)  
or: [security@aims.edu](mailto:security@aims.edu)
- Website: [Weldsheriff.com](http://Weldsheriff.com)

Thank you

