

Common Cents – Protect Your Finances



Solve the Money Mystery

If you become a victim, you may spend a large amount of time closing compromised accounts, opening new accounts and fixing credit records. There can be out-of-pocket expenses related to clearing your name. You could even be denied loans because of identity theft.

How it Happens

Cyberattacks – thieves hack systems, software, and servers in companies of all sizes. They may use the information to open accounts, make charges, or impersonate the business.

Dumpster-diving – thieves can rummage through trash, looking for bills or other papers with your personal information on them.

Identity theft – your name, Social Security number, bank account information, or credit card number used without your permission.

Imposter scams – thieves try to convince you to send money by pretending to be someone you know or trust.

Mail fraud – thieves may send letters asking you to send money or personal information.

Phishing – a scammer tries to trick you into giving out your personal information, such as passwords, credit card numbers, or bank account information.

Skimming – thieves can steal credit/debit card numbers by using a special storage device when processing your card.

Spoofing – a caller disguises the information shown on your caller ID.

Wire or money transfer fraud – thieves try to trick consumers into wiring or transferring money to them.

What can I do?

Don't talk to strangers. Don't give out personal information unless you know who you are dealing with. Never click on links sent in unsolicited e-mails.

Protect your Social Security number. Don't carry your Social Security card in your wallet or write the number on a check.

Get creative. Don't use obvious passwords like your birth date, your mother's maiden name or your Social Security number.

Use security questions to verify your account. Examples of security questions are: What was your maternal grandmother's first name? What was the name of your first pet?

Set up roadblocks online. Log out of accounts and close browsers. Use firewalls, spyware and anti-virus software. Update frequently.

Allow notifications for log-in alerts. This can help you know if someone else is trying to access your account.

Shop at reputable businesses in-person or online. Keep records/receipts of your transactions.

Limit the cards you carry. If a card-reading device looks as if it's been tampered with, don't swipe your card.

Hide it. Keep personal information in a secure place at home, especially if you have roommates, employ outside help or are having work done in your house. Shred financial documents, paperwork, and mail with personal information before you discard them.

Monitor accounts and your credit report. View account information online and/or sign up for text alerts. Check your credit report at www.annualcreditreport.com. Contact the bank, credit union, creditor(s), and/or credit bureau(s) if you notice anything suspicious.



Signs that you may be a Victim of Identity Theft.

If you check any of the indicators below, you may be a victim of identity theft:

☐

Are there charges or bills from creditors or collection agencies demanding payment for items that you never bought or for accounts that you never opened?

☐

Is there information in your credit report about accounts that you never opened?

☐

Are there calls from creditors, or potential creditors, about suspicious new accounts, a large volume of credit card activity, wire transfers, etc.?

☐

Have there been unauthorized withdrawals from your bank accounts?

☐

Has your wallet, purse, laptop, iPad or cell phone been lost or stolen?

☐

Are your statements, bills, or other regular mail not arriving on time as regularly scheduled?
(Your mail may have been diverted to another address or stolen from your mailbox.)

☐

Have you had a surprise credit score drop or denial of loan or credit applications?

Contributors

FCS Agents who assisted with the previous Money Talks series and The Great Money Mystery series; Megan Wells, M.S., Program Associate University of Arkansas System Division of Agriculture Cooperative Extension Service.

Author

Laura Hendrix, Ph.D., Accredited Financial Counselor®, Associate Professor – Personal Finance, University of Arkansas System Division of Agriculture Cooperative Extension Service.

References

Federal Trade Commission Consumer Advice, <https://consumer.ftc.gov/>
Consumer Financial Protection Bureau, Fraud and Scams, <https://www.consumerfinance.gov/consumer-tools/fraud/>
[USA.gov](https://www.usa.gov/scams-and-fraud) Fraud and Scams, <https://www.usa.gov/scams-and-fraud>