2015

# 101 Proactive Things You Can Do Right Now to Avoid Identity Theft (especially from cyberspace)

Don P. Diffine Ph.D.
*Harding University*, ddiffine@harding.edu

# 101 Proactive Things You Can Do Right Now To Avoid

# IDENTITY THEFT

## (especially from cyberspace)

Courtesy of
The Belden Center
for
Private Enterprise Education
D.P. Diffine, Ph.D., Director
HARDING UNIVERSITY
Searcy, Arkansas

A
Commemorative Issue
of

The Entrepreneur

a Journal of the

Belden Center for
Private Enterprise Education

Research Assistants and Editors:
Brenda Davis and Maci Handy

Third Edition


Printed by
Harding Press



D. P. Diffine
Harding University
Box 12245
Searcy, Arkansas 72149-0001
ddiffine@harding.edu
(501) 279-4470

*"Identity Theft," affecting one in four American households, is one of the fastest growing crimes in America. Called a low-risk, high reward endeavor by criminals ($55 billion a year), there are many things you can do right now to prevent it.*

*Consider taking some steps to avoid the loss of your personal identity numbers (e.g. Social Security numbers, birth date, credit card numbers, etc.). Your credit record can become as secure as possible.*

*Remember — In financial matters, it is easy for someone to pretend to be you. It then becomes quite frustrating to even prove that you are you! Worst case, it could possibly take agonizing hours, weeks, or months to undo the damage. Most identity theft is fairly low-tech; so are most solutions. Implement them, and sleep well (ok, better).*

## DON'T BE A VICTIM!

To protect yourself from identity theft, remember:


Be **STINGY** about giving out personal information.


**CHECK** your financial and credit card statements as soon as they come in, and make sure they're all accounted for.


**ASK** for your credit report and review it carefully. You are entitled to one free report a year

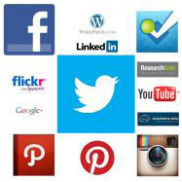

**MAINTAIN** records of your financial, purchasing, and other official activities for at least one year—longer, if possible—and

Source: U.S. Department of Justice

1. Educate yourself on how to be responsible with your money. The American Financial Services Association (AFSA) Education Foundation offers free online courses at *https://www. afsaef.org/*.

2. Social media has made it easier for scammers to gain access to your personal information.

3. Be sure that you know well your friends or followers on social media and that only your friends or followers can see your posts.




4. Be extra careful of what you post. Remember--what you post could still be seen forever, especially if someone saves it as a screenshot.

5. Scammers can save your posts about where you've been and who you've been with. They can use information like this to make you or others think that they really know you.

6. Deactivating your account allows you to temporarily discontinue use of a certain social media. While this prevents others from viewing your personal information, keep in mind that the stored data remains accessible to hackers.

7. To permanently discontinue use of a certain social media, delete your account. Your personal information will be permanently removed from deleted accounts.

8. Increase your privacy settings, for added security.

9. Use strong passwords. Do not use your Social Security number, birth date, mother's maiden name, or other personal information as a password.

10. Change your passwords frequently, and don't use the same password for multiple sites.

11. Never click on the "remember my password" button.

12. When purchasing online, make sure you are using a secure site. Secure sites have a URL that begins with https://.

13. Make online purchases with a credit card, not a debit card, whenever possible. If there is a problem with the transaction, or the debit card gets hijacked, the charges may be disputed and rejected.


14. Try to own a separate credit card specifically used for online purchases.

15. In case something goes wrong with an online purchase, you can cancel that card, while still using your other credit card(s).

16. Don't give personal information over the telephone, through the mail, or internet, unless you have initiated the contact yourself.

17. Download programs only from websites you know and trust.

18. Many bogus programs look real and yet are cyber fraud "phishing" attempts to scoop up your personal identity numbers.

19. Avoid illegal service providers advertising themselves as legitimate legal aid organizations. Legitimate groups require a written retainer agreement before payment.

20. Beware. Capturing millions of identity numbers at one time, cyber fraud terrorists, passing as business customers, can attack unencrypted data brokers' customer databases. Few states are required to report this.

21. Scammers can also pose as a familiar organization. Be wary when a business or agency that you are already a member of asks for you Social Security number or other private information.

22. If you are already a member of an organization, they won't ask for information they already have.

23. Do be suspicious of a call or e-mail saying that he/she is from your bank or credit card company and needs to update your security and/or billing information. Financial institutions don't usually operate that way.

24. If you answer a scammer's call, "pressing any key" even to "opt out" tells them that your number is working and available to them. Only press the "end call" button.

25. Offered free access to an Internet site? Be skeptical.

26. Some scammer's dialer spyware programs bypass local Internet access phone numbers and use an international number for which you are charged.

27. Be picky. Don't connect to just any public Wi-Fi network.

28. Clear the history on your computer regularly.

29. Keep important, personal documents stored on a USB thumb drive instead of directly on your computer. This can help prevent hacking.

30. Before getting rid of your old computer, use hard drive shredding software, or remove and destroy hard drives before discarding the personal computer.

31. Slow yourself down when on the internet. Think before you click on every link that pops up on your screen or in your e-mail.

32. Even if an e-mail appears to be from your financial institution, don't click on the link in your e-mail to access your account. Go to the institution's actual site to log in. This will help avoid phishers.

33. Remove your name from unsolicited mailing lists. E-mail *www.dmachoice. org.*

34. Use *www.optoutprescreen.com/* to get off lists sold by credit reporting bureaus.

35. You can also order a credit report from the following:

    **Equifax**: 800-685-1111
    *www.equifax.com*
    **Experian**: 888-397-3742
    *www.experian.com*
    **TransUnion**: 800-888-4213
    *www. transunion.com*

36. Use Consumer's Union's website *www. defendyourdollars.org* to obtain credit freeze-law details for each of the 50 states.

37. You can request credit reporting services to tag your credit files with a 90-day "*Fraud or Victim Alert*."

38. Call 858-693-7935 or go online to *www.idtheftcenter.org* to get an action plan and a victim impact statement form.

39. File a complaint for fraud involving stolen mail or correspondence online at *https://postalinspectors.uspis.gov/*.

40. Check with *lookstoogoodtobetrue.gov* to stay ahead of the fraudsters' latest scams (e.g. filing fake income tax returns with the IRS for refunds).

41. See the FBI's financial crimes report at *www.fbi.gov/publications.htm*, so that you can be aware of the newest scams and traps and take steps to prevent them from happening to you.

42. Photocopy wallet contents, copying both sides of each credit card. Keep copies and account numbers in a secure place, where you and/or your representative can quickly access them.

43. Never carry your Social Security card, birth certificate, or passport unless necessary.

44. Never leave important documents, receipts, cards, etc. in an insecure place.

45. Store in a safe deposit box at the bank, important birth, marriage, and death certificates, passports, copies of your will, healthcare proxy, insurance, IRA and 401k beneficiary designation forms, etc. (i.e. anything you don't want destroyed by natural disaster).

46. Keep income tax returns, supporting documents, bank statements, investment papers, pay stubs, and credit card statements in a file cabinet or file boxes for five (5) to seven (7) years.

47. Save receipts and compare with billing statements, voiding incorrect receipts and destroying all carbons.

48. Shred all old documents, pre-approved credit card applications, and convenience checks.

49. Ask those you do business with not to use your Social Security number as an identifier. Only your employer, banker, and the IRS need it.

50. Do not print your Social Security number or driver's license number on your checks.

51. Don't have openly visible identification on suitcases and briefcases (under a flap is ok).

52. Avoid ATMs in remote or dark places, especially after hours.

53. When using an ATM, shield your account numbers from onlookers.


54. Don't leave behind your ATM card or receipts after a transaction.

55. Never leave identity papers visible. This includes when selling a car, or even using valet parking.

56. Anything left on dashboard, in the glove box, door pocket, or trunk could be read or copied.

57. Sign your new credit cards right away and keep records and receipts in a secure place.

58. Don't leave behind (especially in stores or restaurants) any receipt that has your credit card number on it.

59. Never return (or leave behind) your hotel's card-type room key. Credit information embedded in it could sit in a drawer, tempting scammers, until the room key is reissued.

60. Put "Photo ID Required" or "See ID" next to your signature on the back of your credit cards.

61. Keep your eye on your credit card during transactions; get it back as quickly as possible.

62. Have you received an unexpectedly reissued credit card with a different account number? The issuer may be worried about a possible breach of their customer data base. For clarification, read closely any accompanying information.

63. The more credit cards you have, the more opportunities thieves have to steal from you.

64. Shred all the credit cards you don't use regularly.

65. Be wary of thieves using handheld magnetic card readers to glean information off of the magnetic strip on credit cards and debit cards.

66. Thieves can intercept incoming or outgoing mail, make your minimum payment along with a change of address (to them), and run up your balance until detected.

67. Put trash out the morning of pick-up, instead of the night before.

68. When you are away, have the post office hold your mail. This takes away the chances for ID thieves to rummage through your mail box.

69. Get a mailbox that locks or a post office box, so that scammers can't steal important mail with account information.

70. Take outgoing mail containing personal information directly to the post office.

71. Be cautious when you move. Notify the post office, bank, credit card companies, insurance companies, and healthcare providers seven to ten days before you move.

72. During the move, carefully transport your important documents and account information with you in a locked box.


73. Get a copy of your credit report three months after your move, to verify that no new accounts have been opened in your name.

74. Take your computer with you on a move, instead of letting the movers take it with them.

75. Ordering new checks? Have them sent to the Customer Service department at your bank.

76. Immediately number your deposit slips. Whenever your checkbook has been in someone else's hands, however briefly, check to see if any deposit slips are missing.

77. Clever thieves can take a deposit slip, instead of a check, making it easier for them to pass forged checks.

78. Don't just issue "stop payments" on stolen checks. Instead, cancel the account.

79. Scammers tend to target online shoppers during a busy holiday season. Remember your status or situation at the time.

80. Your socio-economic position of authority and prominence can set you up as a bigger and more available target.

81. Be alert to con artists calling older adults saying a relative is sick, owes money, or is in trouble. Scammers use urgency so that there is no time to verify their fraud.

82. Seniors, an easy way to bond and involve the younger generation is to share information about scams with your family and friends on social media.

83. Be aware, senior citizens, that con artists target you because you are available, often have money, and may be lonely.

84. Con artists can also try to sell fraudulent promissory notes at attractive rates. Don't let yield blind you to risk.

85. Seniors, bond ahead of time with a trusted adult child for these decisions. These trusted relatives can supervise senior family members' finances to spot unusual circumstances, transactions, or withdrawals involving missing checks and funds.

86. Put a "deceased" alert on a deceased relative's credit reports.

87. Do not include the exact month/day/ year birthdate of a deceased relative to be listed in the newspaper obituary column.

88. Inform the Social Security office of a death by taking them a copy of the death certificate.

89. If necessary, file a complaint with *www.elderabusecenter.org*.

90. Check periodically that unauthorized medical procedures and treatments to an unknown person have not been made in your name as fraudulent claim.

91. Don't pay a bill that isn't yours, and don't cover any fraudulent checks.


92. Even if you've notified authorities of fraud, your credit rating may be temporarily adversely affected, but should not be permanently damaged.

93. Remove your name from pre-approved offers and mailing lists (call 888-5-OPTOUT).

94. Have letters placed in credit reporting bureaus' files, specifically asking lenders to contact you directly before granting credit in your name.

95. Order one free credit report a year from *annualcreditreport.com* or call 877-322-8228.

96. Phone the institution immediately if your credit card or bank account number was stolen. Follow up with a letter.

97. Report any crime in writing. Credit grantors and insurance companies often require a police report to verify the crime (even though some police departments consider these low priority and may resist).

98. Report fraud to credit card issuers. Get new cards with new account numbers requesting that old accounts be processed as *"Account closed at customer's request."*

99. Contact FTC's Identity Theft Hotline (877-438-4338, *www.consumer.ftc.gov/*) for an "ID Theft Affidavit," to notify merchants, financial institutions, and credit bureaus.

100. If your Social Security number is compromised, and you know or suspect you are a victim of tax-related identity theft (i.e. they file before you can, and steal your money!), complete and submit IRS Form 14039.

101. Parents, be vigilant! Young people are especially vulnerable: trusting; financial documents not always secured; careless online; liberal file sharing; good credit histories; unlikely to read bank statements closely; and not yet prone to order credit reports. Trust but verify.

## POST SCRIPT

A book that caught the compiler's eye late in the development of this publication was Stealing Your Life in 2007. The author, Frank Abagnale, was played by Leonardo DiCaprio in the 2002 biographical crime drama film *Catch Me If You Can*, also featuring Tom Hanks.

## ACKNOWLEDGMENTS

Special thanks go to the office manager, Brenda Davis, and student workers, Maci Handy and Aubrey Hitt for their perseverance with me, especially on matters of form and style. They have made every effort to include only relevant, verifiable, reliable text. May their tribe increase.

## ORGANIZATIONS AND WEBSITES

**Anti-Phishing Working Group (APWG)**: A worldwide coalition that unifies the global response to cybercrime across different sectors, focused on eliminating identity frauds that result from growing email spoofing, crime ware and phishing. *www.antiphishing.org/*

**Fight Identity Theft**: An organization that does exactly what their name says--fight identity theft by focusing on three main categories of identity fraud: protect, detect and recover. In these sections they cover tips, and guidelines to identity theft. *http://www.fightidentitytheft.com/*

**Identity Theft Resource Center**: Covers all forms of ID theft--criminal, financial, medical, government and more, offering free victim assistance to consumers in the United States. They also strive to educate individuals, businesses and agencies about identity fraud and serve to be a source of information regarding this issue. *http://www.idtheftcenter.org/*

**Medical Information Bureau**: Maintains information, tips and tools for consumers targeted to identity theft related to medical fraud. *http:// www.mib.com/medical_identity.html*

**National Consumers League**: The oldest consumer organization in America, providing press releases, blogs and news articles on the hot topic of identity theft. *http://www.natlconsumersleague.org*

**Privacy Rights Clearinghouse**: A great resource of information on identity theft and almost every related topic including finance, data breaches, insurance, online privacy, Social Security numbers, junk mail and more. Also included are interactive tools to help gauge your likelihood of becoming a victim. *https://www.privacyrights.org/*

**On Guard Online**: *A*n educational guide on how to prevent identity theft and internet fraud, compiled by contributors in the federal government and the technology industry. A very useful site for individuals seeking tips on how to secure their computer. *www.onguard online.gov*

**Two helpful links** on deactivating and deleting social media accounts provide tips, and the pros and cons of deactivating and deleting accounts. *http://mashable.com/2013/03/01/ delete-your-facebook-account/ https://www. facebook.com/help/359046244166395/*

## ADDITIONAL REFERENCES


Abagnale, Frank. Stealing Your Life. Broadway Books, 2007.

Acohido, Byron. *Meet A-Z: He's Behind a Cybercrime Wave*. *USA Today*. August 5, 2008.

Anderson, Nancy. *The Best Form of Identity Theft Protection No One Knows About. Forbes.* July 15, 2015.

Anderson, Nancy. *7 Things You Can Do to Ward Off Identity Theft. Forbes.* June 13, 2015.

Balakrishnan, Anita. *Tips on What to do if You've Been Hacked*. *USA Today*. August 7, 2015.

Beherec, Sean and Chad Day. *Survey: ID Theft up 34% since '05*. *Arkansas Democrat Gazette*. December 1, 2011.

Bertagnoli, Lisa. *7 Tips for Using Budgeting Apps Safely. TIME.* August 7, 2015.

Blomeley, Seth. *Leaders Get Ideas to Fight ID Theft*. *Arkansas Democrat Gazette*. July 26, 2006.

Browne, Andrew. *Think ID Theft Can't Happen to You? Think Again*. *SC Magazine*. May 21, 2012.

Chu, Kathy. *Feds accuse CompuCredit of Deceiving Customers*. *USA Today*. June 11, 2008.

Collins, Keith. *Here's Why Companies Keep Losing the Battle Against Hackers*. *Businessweek*. July 15, 2015.

*Cybercrime: Thieves in the Night. The Economist.* December 17, 2014.

*Cyber-Crime and Business: Think of a Number and Double It. The Economist.* January 17, 2015.

Dadisho, Ed. *Identity Theft and the Police Response: The Problem*. *Police Chief Magazine.*

Freudenheim, Milt. *Old, Trusting, and Tricked Out of Life Savings. The New York Times.* September 11, 2012.

Guest, James. *Protect Yourself Online*. *Consumer Reports*. September 2008.

Guest, James. *Protect Your Privacy Online*. *Consumer Reports*. June 2012.

Henig, Samantha. *Proving You're You*. *Newsweek*. March 12, 2007.

Huffman, Mark. *'Farcing' Overtaking 'Phishing' as Online Identity Theft Threat. Consumer Affairs.* August 6, 2014.

Kirchheimer, Sid. *R.I.P. Off*. *AARP Bulletin*. June 2015.

Kirchheimer, Sid. *10 Ways to Prevent Identity Theft When Travelling*. *AARP Bulletin*. July 10, 2015.

Kirchheimer, Sid. *Your Personal Data, Up for Grabs*. *AARP Bulletin*. February 2015.

Lawrence, Dune. *An Identity Thief Explains the Art of Emptying Your Bank Account*. *Businessweek*. July 15, 2015.

Levin, Adam. *Not so FAFSA: How to Avoid a Student Aid Scam*. *ABC News*. August 2, 2015.

Marbaix, Jill Rachlin. *Lessons in Privacy*. *U.S. News & World Report*. September 6, 2004.

McCoy, Kevin. *Identity Thieves Tax the System*. *USA Today.* April 11, 2008.

Miller, Michael E. *'Car Hacking' Just got Real. The Washington Post.* July 22, 2015.

*Nation's Leading Identity Theft Protection Service Can Help Protect You from One of America's Fastest Growing Crimes*. *USA Today.* July 11, 2008.

Nelson, Daryl. *Is Identity Theft Unavoidable?. Consumer Affairs.* March 18, 2013.

Risen, Tom. *Identity Theft Remains Top Threat. U.S. News & World Report.* March 2, 2015.

Schmidt, Michael, David Sanger, Nicole Perlroth. *China Hackers Target Data on U.S. Workers*. *Arkansas Democrat Gazette*. July 10, 2014.

Swartz, Jon. *Credit Lockdown Privileges Spread*. *USA Today*. October 4, 2007.

*Swiped, Stolen, and Sold*. *The New York Times.* August 6, 2008

U.S. News Staff. *10 Signs You Might be a Victim of Identity Theft. U.S. News & World Report.* July 7, 2015.

Walker, Danielle. *Medical Identity Theft to be Explored at FTC Hearing*. *SC Magazine*. May 3, 2013.

Weise, Elizabeth. *Hackers' Targets Growing in Scope*. *USA Today*. August 6, 2015.

Weston, Liz. *The Care and Feeding of Your 401(k). AARP Bulletin*. April 2015.

Wildstrom, Stephen H. *Tech and You. Businessweek*. March 2008.

Yancey, Kitty Bean. *Swipe that Debit Card Carefully*. *USA Today.* March 13, 2008.

## ABOUT THE COMPILER

In his 45th year, Dr. Don Diffine is currently Professor of Economics at Harding University in Searcy, Arkansas, Founding Director of the Belden Center for Private Enterprise Education and Senior Research Associate of Harding's American Studies Institute (ASI). Dr. Diffine is listed in the Heritage Foundation's Guide to Public Policy Experts.

Dr. Diffine has provided Congressional testimony on business problems, economic impact statements, and inflation-recession dilemmas. He is a member of the Governor's Council of Economic Advisors and presently has 11 books and 25 monographs in print.

Diffine has served on the Board of Directors of the Arkansas Council of Economic Education, as a member of the International Platform Association, and has spoken frequently for conventions, management clubs, stock-holders' meetings, trade associations, and chambers of commerce.

A former United States Air Force Captain and Squadron Commander during the Vietnam era, Diffine's formal education includes a Bachelor's Degree in Economics from California State University at Long Beach, Master's Degree in Economics from St. Mary's San Antonio, Texas, and a PhD from the University of Mississippi.

He also received two in-residence fellowships from the Foundation for Economic Education, Irvington-on-Hudson, New York. His Adjunct Professor stints include Pepperdine University, Webster University, University of Arkansas at Little Rock, Arkansas State University and the Mid-South School of Banking.

The recipient of the $7,500 Freedoms Foundation Principle Award for Excellence in Private Enterprise Education, Dr. Diffine has received 16 additional Freedoms Foundation awards in the

categories of Non-profit Publications, Economic Education, Public Affairs-Advertising, Public Address, and Published Works. Recipient of the National Flag Foundation's New Constellation Award, he is also the faculty winner of a $1,000 First Place prize in a National Essay Contest judged by Nobel economist Milton Friedman.

In 2000, Diffine was inducted into the Samuel Moore Walton Free Enterprise Hall of Fame. In 1995, he received the Champion of Enterprise award and became the first inductee into the National Students In Free Enterprise Hall of Fame in Kansas City. The First Annual Distinguished Scholar Award was also presented in 1988 to Dr. Diffine in Cleveland, Ohio, by the Association of Private Enterprise Education.

Dr. Diffine has been married for 51 years to the former Dion Hillman of Kailua, Hawaii, a retired math teacher from the Searcy Public Schools. The Diffines have two children: David, who is a medical doctor, and Danielle, who is an accountant. Six wonderful grandchildren round out the family tree: Katie Elizabeth; Ridge Tyler; Lillie Ann; Piper Dion, Emery Rayne, and Gatlyn Sayge.