Ann Cowan Dixon Archives & Special Collections

Harding University
Scholar Works at Harding

Belden Center Monographs

The Belden Center for Private Enterprise Education

2008

50 Proactive Things You Can Do Right Now to Avoid Identity Theft (Especially from Cyberspace)

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

Follow this and additional works at: https://scholarworks.harding.edu/belden-monographs

Recommended Citation

Diffine, D. P. (2008). 50 Proactive Things You Can Do Right Now to Avoid Identity Theft (Especially from Cyberspace). Retrieved from https://scholarworks.harding.edu/belden-monographs/56

This Book is brought to you for free and open access by the The Belden Center for Private Enterprise Education at Scholar Works at Harding. It has been accepted for inclusion in Belden Center Monographs by an authorized administrator of Scholar Works at Harding. For more information, please contact scholarworks@harding.edu.

HARDING UNIVERSITY

"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. Read on, please.

1. Photocopy wallet contents copying both sides of each credit card. Keep copies and account numbers in a secure place.
2. Store in a fire-proof box, or 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.
3. Keep income tax returns, supporting documents, bank statements, investment papers, pay stubs, credit card statements in a file cabinet or file boxes for seven (7) years.
4. Never carry your Social Security card, birth certificate, or passport unless necessary.
5. Do not use your Social Security number, birth date, mother's maiden name or other personal information as a password.
6. Ask those you do business with not to use your Social Security number as an identifier. Only employer, banker, and IRS need it.
7. Do not print your Social Security Number or drivers license number on your checks.
8. Never leave important documents, receipts, cards, etc. in an insecure place.
9. Don't have openly visible identification on suitcases and briefcases.
10. Never leave anything out with your address visible. This includes when selling a car, or even using valet parking. Anything left in the glove box could be read or copied.
11. When using an ATM, shield your account numbers from onlookers. Don't leave behind ATM card or receipts after a transaction. Avoid ATMs in remote or dark places.
12. Save receipts and compare with billing statements, voiding incorrect receipts and destroying all carbons.
13. Sign your credit cards right away; keep records and receipts in a secure place. 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.
14. Keep your eye on your credit card during transactions; get it back quickly as possible.
15. Be wary of thieves using handheld magnetic card readers (that can be bought on the Internet) to glean information off of the magnetic strip on credit cards and debit cards.
16. Put trash out the morning of pick-up, instead of the night before.
17. Use a secure U.S. Postal Service mailbox for outgoing and incoming mail.
18. Notify credit card companies in advance of address change. 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.
19. Don't give personal information over the telephone, through the mail, or Internet unless you have initiated the contact.
20. Create passwords for your accounts. Never repeat a previous password you have used.
21. Avoid illegal service providers advertising themselves as legitimate legal aid organizations. Legitimate groups require a written retainer agreement before payment.
22. Ordering new checks? Have them sent to the bank. Don't just issue "*stop payments*" on stolen checks. Instead, cancel the account.
23. 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.
24. Download programs only from websites you know and trust. Many bogus ones look real and yet are cyber fraud "phishing" attempts to scoop up your personal identity numbers.
25. Beware. Capturing millions of identity numbers at one time, cyber fraud terrorists passing as business customers can attack unencrypted data broker's customer databases. Only California is required to report this.
26. Offered free access to an Internet site? Be skeptical. Some scammer's dialer spyware programs bypass local Internet access phone number and use an international number for which you are charged.
27. Before getting rid of your old computer, use hard drive shredding software, or remove and destroy hard drives before discarding the personal computer.
28. Be very diligent about shredding any old documents, pre-approved credit card applications, and convenience checks.
29. Remove your name from pre-approved offers and mailing lists (call 888-5-OPTOUT).
30. Remove your name from unsolicited mailing lists. Write to *Direct Marketing Association's Mail Preference Service*, P.O. Box 9008, Farmingdale, NY 11735.
31. Use *optoutprescreen.com* to get off lists sold by credit-reporting bureaus.
32. Have letters placed in credit reporting bureaus files, specifically asking lenders to contact you directly before granting credit in your name.
33. Order one free credit report a year from *annualcreditreport.com* or call 877-322-8228.
34. Order a credit report from the following: Equifax's (800-685-1111, *www.equifax.com*); Experian (888-397-3742, www.*experian.com*); or TransUnion (800-680-7293, *www.transunion.com*).
35. Use Consumer's Union's website *financialprivacynow.org* to obtain freeze-law details for each of the 50 states. You can request credit reporting services tag your credit files with a 90-day "*Fraud or Victim Alert*".
36. Check periodically that unauthorized medical procedures and treatments to an unknown person have not been made in your name as a fraudulent claim.
37. Don't pay a bill that isn't yours, and don't cover any fraudulent checks. If you've notified authorities, your credit rating should not be permanently affected.
38. Phone the institution immediately if your credit card or bank account number was stolen. Follow up with a letter.
39. Do report any crime in writing. Credit grantors and insurance companies often require a police report to verify the crime.
40. 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.*"
41. Contact FTC's Identity Theft Hotline (877-438-4338,www.consumer.gov/idtheft) for an "ID Theft Affidavit," to notify merchants, financial institutions, and credit bureaus.

42. Call 858-693-7935 or go online to *www.idtheft-center.org* to get an action plan and a victim impact statement form.
43. Consider filing a complaint for fraud involving stolen mail and correspondence. Contact *www.usps.com/postalinspectors/fraud/mailfraudcomplaints.htm.*
44. Check with *www.snoopes.com* and lookstogoodtobetrue.gov to stay ahead of the fraudsters latest scams (e.g. filing, fake income tax returns with the IRS for refunds). See FBI's financial crimes report at *www.fbi.gov/publications.htm.*
45. Be aware, senior citizens, that con artists target you because you are available, often have money, and may be lonely. They try to sell fraudulent promissory notes at attractive rates. Don't let yield blind you to risk.
46. Never allow the birthdate of the deceased to be listed in the newspaper obituary column.
47. Bond ahead of time with a trusted adult child for these decisions. Supervise senior family members finances to spot unusual circumstances, transactions, withdrawals involving missing checks and funds. File complaint with elderabusecenter.org.
48. Be alert to con artists calling older adults saying a relative is sick, owes money, or is in trouble. These scammers use urgency so that there is no time to verify their fraud.
49. 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.
50. 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 up credit reports.

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 lo-tech; so are most solutions. Implement them, and sleep well (ok, better).

Harding University
Belden Center for Private Enterprise Education
Box 12245
Searcy, Arkansas 72149-2245

NON PROFIT ORG.
U.S. POSTAGE
PAID
PERMIT No. 22
SEARCY, ARK.
72143

50 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