Generic Identity Theft Web Site (Section Five)

Other Toolkit Sections

Toolkit Home | Section 1: Building a Press Release | Section 2: Notification Letter Components | Section 3: Incident-Specific Web Site Template | Section 4: Incident Response FAQ

Generic Identity Theft Web Site Template Instructions

Use this template to create a generic identity theft Web site to be perpetually published as a public service announcement to your institution's community. It can subsequently be linked from any incident-specific site.

Make sure to verify that contact information is correct at the time you publish and review all content for application to your institution and location.

There are many excellent resources and sources whose primary purpose is to educate the community at large about identity theft and preventive measures. The following template pulls from those sources and from the public Web sites of many institutions of higher education. The template includes information about the most important aspects of the topic like what it is, how to protect yourself, and what to do if you become a victim but omits other aspects that are covered by the resources linked in the resources section like how does it most frequently occur and what are the most common crimes committed. Thus the generic Web site template does not attempt to recreate all of the available information; rather, it provides a general overview.

Template

Introduction

This site contains information on how to protect yourself from identity theft as well as what to do to if your personal information becomes exposed or if you actually become a victim of identity theft. Links to additional information can be found under Resources.

What is Identity Theft?

Identity theft occurs when someone uses another person's personal information such as name, Social Security number, driver's license number, credit card number, or other identifying information to take on that person's identity in order to commit fraud or other crimes.

How to Protect Yourself from Identity Theft

The following tips can help lower your risk of becoming a victim of identity theft.

1. **Protect your Social Security number.** Don't carry your Social Security card or other cards that show your SSN. Read "Your Social Security Number: Controlling the Key to Identity Theft" and "Identity Theft And Your Social Security Number".
2. **Use caution when giving out your personal information.** Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails, and in postal mail. Most institutions wouldn't ask for your SSN or other personal information over the phone, and many emphasize that they do not ask for this information. Do not send your SSN or credit card information via email. If you wouldn't feel comfortable putting this information on a postcard, you probably wouldn't want to send it by email either.
3. **Treat your trash carefully.** Shred or destroy papers containing your personal information including credit card offers and "convenience checks" that you don't use.
4. **Protect your postal mail.** Retrieve mail promptly. Discontinue delivery while out of town.
5. **Check your bills and bank statements.** Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.
6. **Check your credit reports.** Review your credit report at least once a year. Check for changed addresses and fraudulent charges.
7. **Stop pre-approved credit offers.** Pre-approved credit card offers are a target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call toll-free 888-5OPTOUT (888-567-8688).
8. **Ask questions.** Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. If you're not satisfied with the answers, don't give your personal information.
9. **Protect your computer.** Protect personal information on your computer by following good security practices.
    - Use strong, non-easily guessed passwords.
    - Use firewall, anti-virus, and anti-spyware software that you update regularly.
    - Download software only from sites you know and trust and only after reading all the terms and conditions.
    - Don't click on links in pop-up windows or in spam e-mail.
10. **Use caution on the Web.** When shopping online, check out a Web site before entering your credit card number or other personal information. Read the privacy policy and take opportunities to opt out of information sharing. Only enter personal information on secure Web pages that encrypt your data in transit. You can often tell if a page is secure if "https" is in URL or if there is a padlock icon on the browser window.

Steps to Take if Your Data Becomes Compromised or Stolen

Credit Reporting Agencies

If you have reason to believe your personal information has been compromised or stolen, contact the Fraud Department of one of the three major credit bureaus listed below. Individuals whose personal information was involved in this incident can request a free initial (90 day) fraud alert to be placed on their credit files by calling any one of the three major national credit bureaus or completing an online form. Submit one online form request and all three agencies will add the fraud alert.

- Equifax
  Direct Line for reporting suspected fraud: 800-525-6285
  Fraud Division
  P.O. Box 740250
  Atlanta, GA 30374
  800-685-1111 / 888-766-0008
  http://www.equifax.com

- Experian
  Direct Line for reporting suspected fraud:
  888-397-3742
  Credit Fraud Center
  P.O. Box 1017
  Allen, TX 75013
  888-EXPERIAN (888-397-3742)
  http://www.experian.com

- Trans Union
  Direct Line for reporting suspected fraud:
  800-680-7289
  Fraud Victim Assistance Department
  P.O. Box 6790
  Fullerton, CA 92634
  Phone: 800-916-8800 / 800-680-7289
  http://www.transunion.com

When contacting the Credit Reporting Agency, you should request the following:

1. Instruct them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.
2. Ask them for copies of your credit report(s). (**Credit bureaus must give you a free copy of your report if it is inaccurate because of suspected fraud.**) Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. **NOTE:** In order to ensure that you are issued free credit reports, we strongly encourage you to contact the agency's **DIRECT LINE (listed above) for reporting fraud**. We do not recommend that you order your credit report online.
3. You may want to ask about the option to freeze your credit. Forty-seven states and the District of Columbia have enacted legislation allowing consumers to place "security freeze" on their credit reports. A consumer report security freezes limits a consumer reporting agency from releasing a credit report or any information from the report without authorization from the consumer. Check your state's information.
4. Be diligent in following up on your accounts. In the months following an incident, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.
5. If you find that any accounts have been tampered with or opened fraudulently, close them immediately. To ensure that you do not become responsible for any debts or charges, use the ID Theft Affidavit Form developed by the Federal Trade Commission (FTC) to help make your case with creditors.

You may request a free annual credit report, 1 per year, from AnnualCreditReport.com as recommended by the Federal Trade Commission.

Social Security Administration
SSA Fraud Hotline: 800-269-0271
http://www.ssa.gov/

If you are the victim of a stolen Social Security number, the SSA can provide information on how to report the fraudulent use of your number and how to correct your earnings record. We encourage you to contact the SSA Fraud Hotline immediately once you suspect identity theft.

The website also provides tips on using and securing your Social Security number. Visit the SSA website for advice on keeping your number safe.

ID Theft Clearinghouse
1-877-ID-THEFT (1-877-438-4338)

Call the ID Theft Clearinghouse toll free at to report identity theft. Counselors will take your complaint and advise you how to deal with the credit-related problems that could result from identity theft.

Local Law Enforcement

It is important that you report identity theft to your local police department as soon as you become aware that you are a victim. Get a copy of the police report which will assist you when notifying creditors, credit reporting agencies, and if necessary, the Social Security Administration (SSA).

Resources

The following links provide detailed information related to identity theft and protecting yourself.

- Department of Justice
- Federal Trade Commission
- Social Security Administration
- Privacy Rights Clearinghouse Identity Theft Resources
- National Consumer League's Fraud Center
- Identity Theft Resource Center (888-400-5530)

Contact Us

Questions or comments? Contact us.

Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).