

Deter - Detect - Defend: Avoid ID Theft

By www.ftc.gov/idtheft

The following information was taken from a brochure published by the Consumer Reports Center of the Federal Trade Commission. IS&T would like to thank them for the valuable information on this summary of ID theft.

What is Identity Theft?

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

Common Ways ID Theft Happens:

How can you lose your identity?

1. **Dumpster Diving:** ID Thieves rummage through trash looking for bills or other paper which contains your personal identification.
2. **Skimming:** ID Thieves steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing:** ID Thieves pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address:** ID Thieves divert your billing statements to another location by completing a post office 'change of address' form.
5. **Stealing:** ID Thieves steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records from your employer, or bribe employees who have access.

Deter:

Deter identity thieves by safeguarding your information:

- **Shred** financial documents and paperwork with personal information before you discard them.
- **Protect** your Social Security Number. Don't carry your SSN card in your wallet or write it on a check. Give it out only if absolutely necessary or ask to use another identifier.
- **Don't** give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- **Never click** on links sent in emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit OnGuardOnline.gov for more information.
- **Don't** use an easily-guessed password like any word in a dictionary, your birth date, a number series, your mother's maiden name, the last four digits of your SSN, etc.

- **Keep** your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

Detect:

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

Inspect:

- **Your credit report:** Credit reports contain information about you, including what accounts you have and your bill paying history.
 - The law requires the major nationwide consumer reporting companies – Equifax, Experian, and TransUnion – to give you a free copy of your credit report each year if you ask for it.
 - Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Requesting Service, P.O. Box 105281, Atlanta, GA 30348-5281. There are companies that charge for this service. Do not be fooled by them. You do not have to enter a credit card number or purchase ID fraud insurance to get this information.
- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

Defend:

Defend against ID theft as soon as you suspect it:

- **Place a 'Fraud Alert' on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert: a call to one company is sufficient:
 - Equifax: 1-800-525-6285
 - Experian: 1-888-EXPERIAN (397-3742)
 - TransUnion: 1-800-680-7289

Placing a fraud alert entitles you to free copies of your credit reports. These take fifteen days to receive, so get your free online report **first**. Look for inquiries from companies you haven't

Deter - Detect - Defend, cont.

contacted, accounts you didn't open and debts on your accounts that you can't explain.

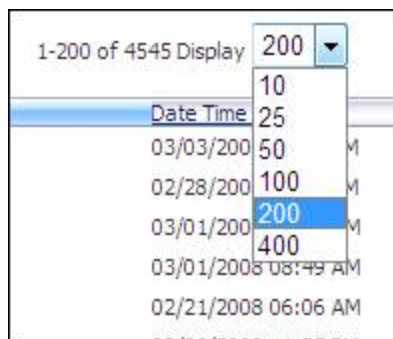
- Close accounts. Close any accounts that have been tampered with or established fraudulently.
 - Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
 - Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
 - Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
 - Keep copies of documents and records of your conversations about the theft.
- File a police report. File a report with law enforcement officials in your city to help you with creditors who may want proof of the crime.
- Report the theft to the Federal Trade Commission. Your report helps law enforcement officials across the country in their investigations.
 - Online: ftc.gov/idtheft
 - By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
 - By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

Anti-spam Tip of the Month

Sorting anti-spam quarantine listing

Recently, one of our professors asked if it was possible to sort the daily quarantined email list by subject. If the emails were sorted by subject, he felt that it would be easier to discard whole blocks of spam emails while looking for the occasional good email that the system considered to be spam, making this tiresome job slightly easier. A little research found this to be possible, but not using the daily email we all receive. Here's how to do it:

- 1) Log onto antispam.csuohio.edu using your CSU ID number and CampusPASS password. This Web site contains your quarantine for the last 30 days as well as your personal anti-spam settings.
- 2) Change the display line count so that it displays, as nearly as possible, current spam only:



I get about 150 spam messages a day so I set my display to show 200 lines.

- 3) Click on 'Subject' or any of the other column titles by which you may want the spam sorted: From, Threat, or Category (Date Time Received is the default sort order).
- 4) Scroll through the sorted spam and find the good messages, if any.

Computational Services Committee

By B. Browning

The Computational Services Committee consists of faculty members along with ex officio participants from the administration and IS&T. The committee meets several times per academic year to assess the information services and technology provided for academic use and to determine the academic needs in this area -- to include the use of software, services, computers and their peripherals, and all computational equipment in faculty research and classroom teaching.

If you have any issues or concerns that you would like to have reviewed by the committee, please email the current chair, Birch Browning from the Department of Music, at b.browning@csuohio.edu. There will likely be only one more meeting this year, so please submit your concerns ASAP.

Quote of the Month

If I believe I cannot do something, it makes me incapable of doing it. But when I believe I can, I acquire the ability to do it, even if I did not have the ability in the beginning.

-Mahatma Gandhi

Editor: F. L. Ferreri, f.ferreri@csuohio.edu or 216-687-2160.

Back issues available online at www.csuohio.edu/ist/info.html - CSU is an Affirmative Action/Equal Opportunity Institution.



2121 Euclid Avenue
RT 1104