



Identity Theft

Officer Jenna Redel
University of Missouri Police Department

Computers as a Crime Tool

- **Computers are becoming more popular with the criminal element**
- **Desktop publishing makes anyone look legitimate**
- **Many prisons are educating convicts in computer technology as part of vocational training**

Criminals adapt and adopt technology

- **Credit card “skimmer”**
- **ATM machines**
- **ID Theft**
- **Viruses**

The internet is moving into more and more homes. (134+ million in the US)

Advantages Computer Provide

- **Expands victim pool and locations**
- **Anonymity**
- **Speed**
- **More and more people do online transactions**
- **Cost**

The Internet

- **300 Million Connected Users**
- **Available worldwide**
- **Internet economy in the US**
 - **Est. 106 million X-mas shoppers in 2001**
 - **\$9.13 billion in sales in 4th quarter of 2000**
 - **\$11.9 billion in 4th quarter in 2001**

Types of Computer Crimes we are Seeing

- **Identity Theft**
- **Counterfeit Documents**
- **Fraud**
- **Computer Viruses**
- **Child Pornography**

What is Identity Theft?

Unlawfully obtaining, possessing, transferring, or using identifying information of another person without the other person's consent and with the intent to harm or defraud another.

Identity Theft Occurs With

- Credit Cards
- Debit Cards
- Convenience Checks
- Loans
- Bank and Investment Accounts
- Utilities

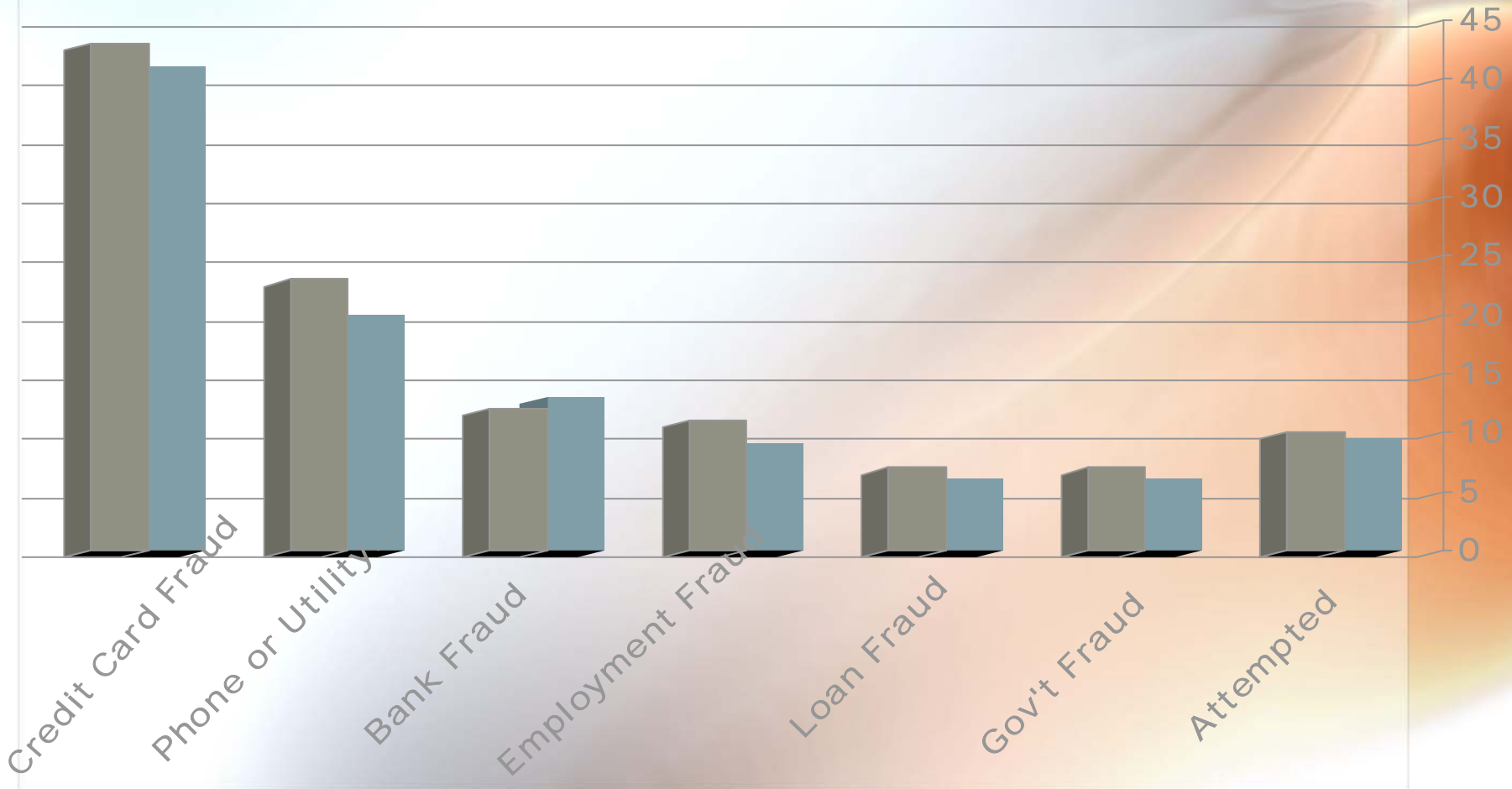
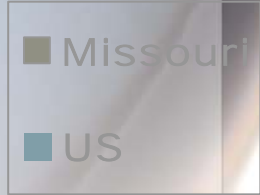


How Big is the Problem?

- **FTC 2003 Survey**
 - **27.3 Million victims within the past 5 years**
 - **10 Million in 2002**
 - **Fastest Growing Crime**
 - **\$48 Billion to business**
 - **\$5 Billion out of pocket**

- **#2 reported crime in 2003**
- **42% of all crime reported to FTC in 2002**
- **55% in 2003**

How Victim's Information Used



•Credit Card Fraud

36,020 Complaints

- New Accounts 26%
- Existing Accounts 19%

•Phone/Utility

17,295 Complaints

- Wireless New 9%
- Telephone New 6%
- Utilities New 3%

•Bank Fraud

11,268 Complaints

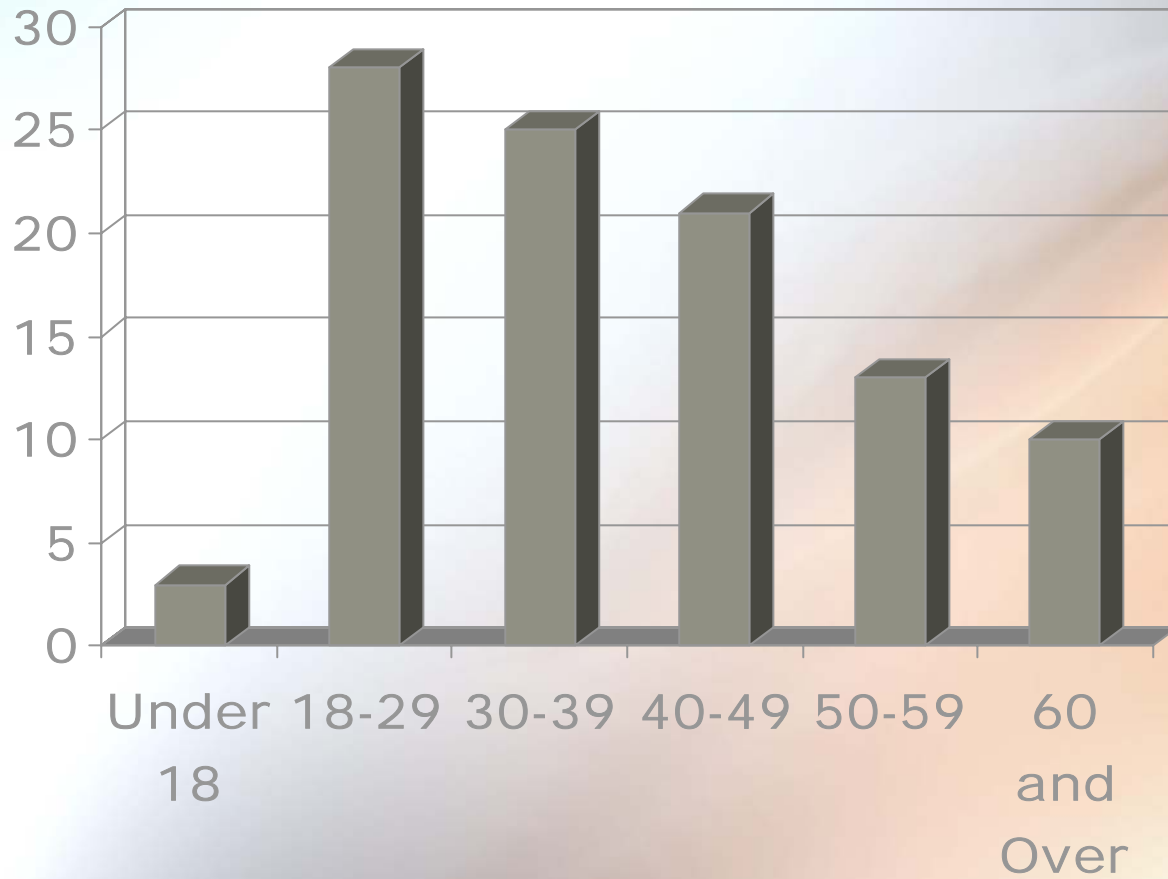
- Existing Accounts 6%
- New Accounts 3%
- Fund Transfers 2%

•Gov't Fraud

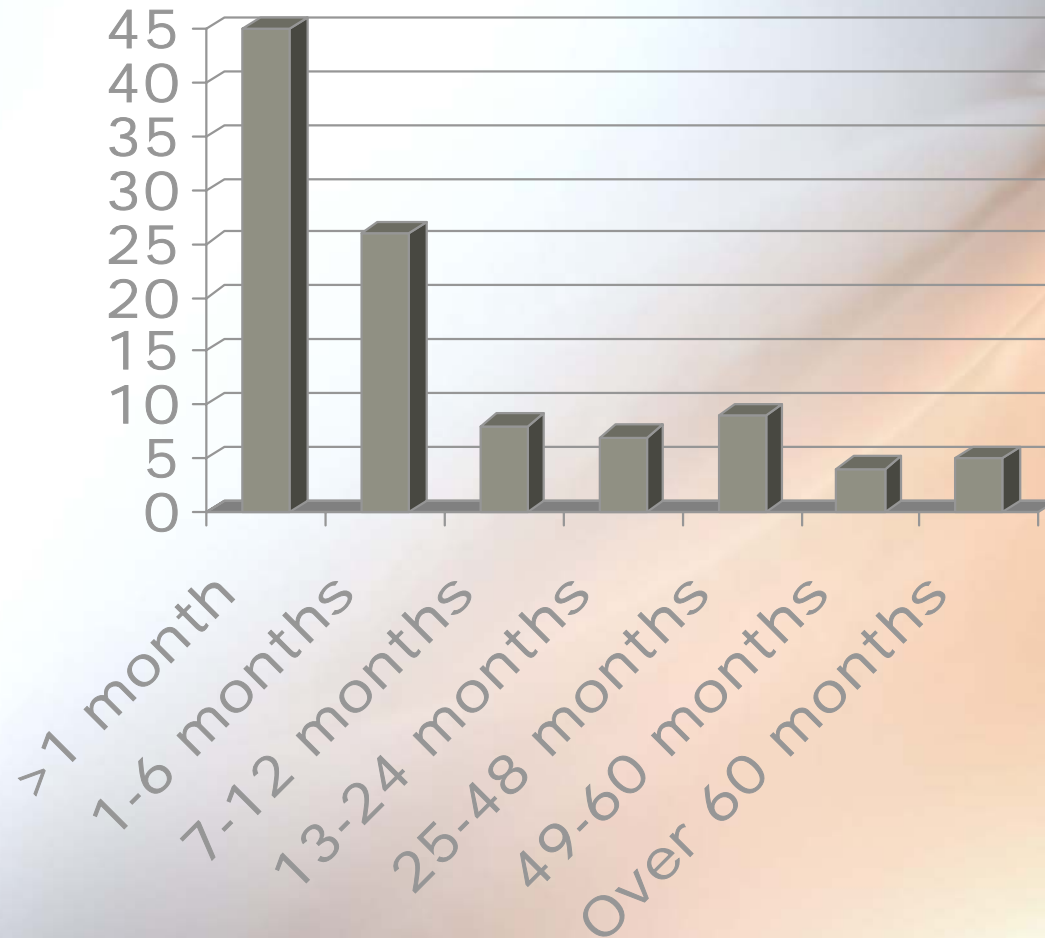
5,380 Complaints

- Driver's Lic 3%
- Tax Return 2%
- SSN Fraud 1%
- Benefits Fraud 1%

Victim's Age Range



Number of Months Between Occurrence and Discovery Date



Who is Stealing Information?

- **Airline Workers**
- **Merchants**
- **Temp Workers**
- **Custodians and Cleaners**
- **Hotel Employees**
- **Restaurant Workers**
- **Postal Employees**
- **Data Entry Workers**
- **Organized Groups**
- **Bank Employees**
- **Prisoners**
- **Telemarketers**
- **Hackers**
- **Health Care Workers**

How Do They Get Information?

- **Stealing Wallets and Purses**
- **Stealing Mail**
- **Trash (2006)**
- **Phishing**
- **Credit Report**
- **Business/Personnel Files**
- **Spoof Websites**

Phishing

- <http://survey.mailfrontier.com/survey/quiztest.html>

How Identity Thieves get Your Personal Information

- In your home
- Internet
- Buy from “inside sources”
- Pen and Paper
- Shoulder Surfing
- Skimming
- Pretexting



What are They Looking For?

- **Credit Cards**
- **Credit Card Statements**
- **Checks**
- **Pre-Approved Credit Card Apps**
- **Convenience Checks**



What Are They Looking For?

- **Credit Bureau Print outs**
- **Bank Statements**
- **Mother's Maiden Name**
- **SSN**
- **Date of Birth**
- **Place of Birth**

What Do They Do With It?

- **Call CC issuer and change address**
- **Open a new CC account**
- **Establish utilities in your name**
- **Open a bank account**
- **Rent apartments**
- **Vehicle loans**

What Else?

- **Go on Spending Sprees**
- **Counterfeit Checks**
- **Give Your Name to Police**
- **Start Over**
- **Cosign Loans**

Identity Theft Types

- **Account Takeover**
- **Fraudulent Applications**

Account Takeover

- **Suspect will obtain personal information of a true person and the Credit Information**
- **Suspect will then change the address on the account by**
 - » **Sending Letter**
 - » **Telephone**
 - » **Fax**

Account Takeover

- **Suspect will usually wait one month to order credit card or checks.**
- **Once they receive the card, the charges begin.**

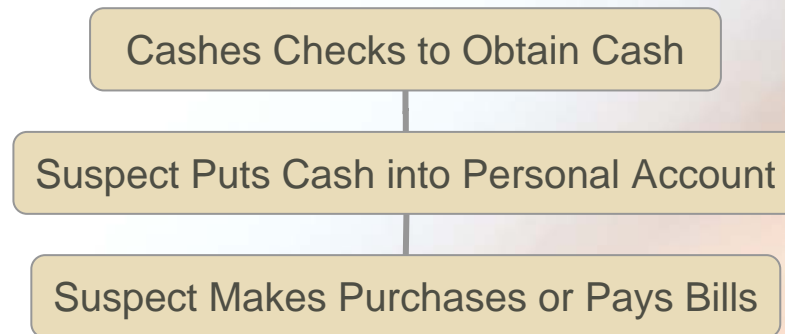
Fraudulent Applications

- **Suspect uses the information of a true person to open a new account by**
 - **Mail**
 - **Fax**
 - **Telephone**
 - **Internet**
 - **Instant Credit**
 - **Add a second person to account**

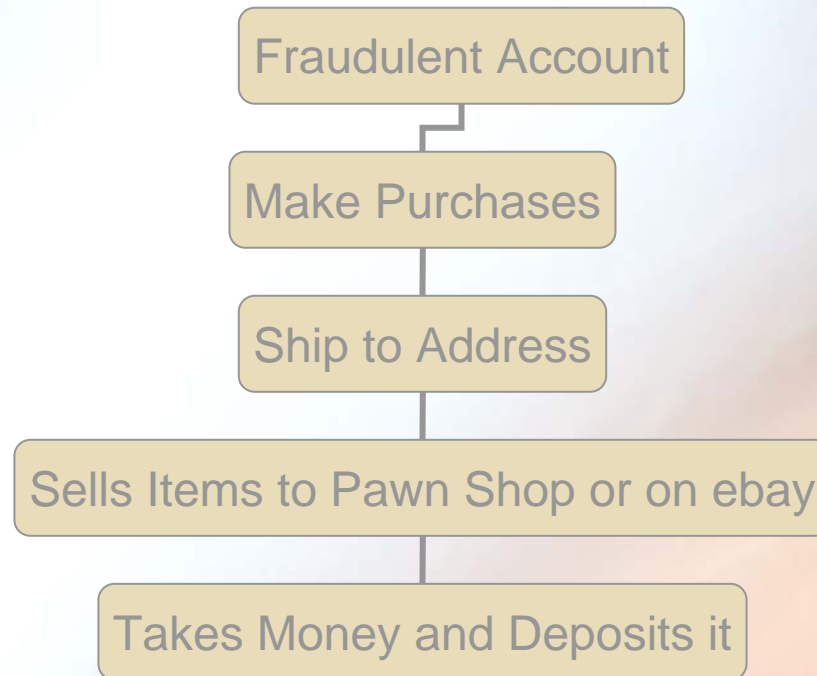
Identity Theft

- **Once the suspect opens the account or taken over the account then they order products**
- **Suspect then has product shipped**
- **Kiting also occurs**

Kiting



Mail Diversion



How to Find Out If You've Been Victimized

- **Obtain Your Credit Report**
- **Closely Check Monthly Statements**
- **You fail to receive bills**
- **You receive CCs you did not apply for**
- **You're contacted by creditors**
- **You're denied credit**

What To Do When ID Theft is Discovered?

- **Contact the Fraud Department**
- **Fraud Alert**
- **Victim's Statement-additional accounts- cell phone #**
- **Check Credit Reports- including inquiries**
- **File a Police Report**

What to do

- **ID Theft Affidavit**
- **Request Letter Stating Account is Closed and Debt Discharged**
- **Keep Detailed Notes of Conversations and Follow Up in Writing- Talk to Fraud Investigator**
- **File an FTC Report**
- **Keep Originals**

Fraud Alerts

- **TransUnion**
 - Initial 12 Months
 - Not Online
 - Free Credit Report
 - Renewal up to 7 years, unlimited
- **Equifax**
 - 6 Months
 - Not Online
 - Free Credit Report
 - Renewal up to 7 years, unlimited

Fraud Alert

- **Experian**
 - **3 Month**
 - **Online**
 - **Free Credit Report on Request**
 - **7 Year Victim Statement**

Credit Reports

- **Up to 9 dollars, 1 free after March '05**
- **Free if inaccurate b/c of fraud**
- **Free if on welfare or unemployed**
- **If turned down for credit/insurance (w/i 60 days)**

Closing Accounts

- **Use new PINS and Passwords**
- **FTC Fraud Affidavit for new**
- **Fraud Dispute Form for existing or sample dispute letter**
- **Close ATM accounts, get new card and PIN**

Checks Washing

- **Checks stolen from unsecured locations**
- **Washed in Acetone**
- **60 minutes**

Stolen Checks

- **Stop Payment**
- **Notify Bank/Verification Service**
- **Banks Require Reasonable Care**

Counterfeit Checks

- **Made at home**
- **Used to buy vehicles**
- **Over payments**

Average Losses

- **Auction Fraud- \$320**
- **Credit Card Fraud- \$120**
- **Investment Fraud- \$570**
- **ID Theft -\$2,000**
- **Check Fraud \$1,100**

Amount Lost

- **Gender**

- Males \$388
- Female \$168

- **Age**

- Under 20 \$270
- 20-29 \$350
- 30-39 \$265
- 40-49 \$260
- 50-59 \$295
- 60 and older \$323

Prevention

- **Credit Card Fraud**
 - Don't give out your CC# online unless a secure site
 - VeriSign
 - Reputable Businesses
 - Physical Addresses
 - Send an Email
 - BBB

Credit Card Fraud

- **Google**
- **Beware of Spam**
- **Don't use Debit Cards Online**
- **Mastercard/ Discover /Citibank**
- **Keep CC info and telephone numbers**
- **Photocopy the contents of your wallet**

Credit Card Fraud

- **Lost/Stolen Wallet Inventory**
- **Give Work Phone Numbers**
- **Recent CC Scam**
- **Don't Give Extra Info**
- **Get a Photocard**
- **Cannot require a minimum purchase**

- **No Extra Charges for CC payment**
- **Do not allow merchants to write your CC# ON CHECKS**
- **Know Your Liability Limits**
- **Don't Store Info on Computer w/o encryption**
- **Install/ Activate Firewalls**
- **Beware on WiFi**

Top 10 Security Tips for Public Hotspots

- **Make sure you're connected to a legitimate access point.** – Don't set to auto connect. Turn off ad-hoc which lets clients cct to you.
- **Encrypt files before transferring or emailing them.** (ex: [Aladdin's Stufft Deluxe](#))
- **Use a virtual private network (VPN).** A VPN establishes a private network across the public network by creating a tunnel between the two endpoints so that nobody in between can intercept the data. ([L2TP/IPSec VPN client](#))
- **Use a personal firewall.** (ex: [ZoneAlarm](#))
- **Use anti-virus software.**

- **Update your operating system regularly.**
- **Be aware of people around you.**
- **Use Web-based email that employs secure http (https).**
- **Turn off file sharing.**
- **Password-protect your computer and important files.**

Don't get pulled in

- **Religious Chat Rooms**
- **Nigerian Scams**
- **Car sales**
- **Investing**
- **Book by it's cover**
- **ID Theft Protection**

Beware

- **Public Computers Pose Risks**
- **Keylogging**
- **Spyware (Adaware Spybot WormGuard Pest Patrol)**
- **WebBugs**
- **PornDialers**





Without



With



From: "Ty Laska" <tylaska@comcast.com>
To: "Scott" <scott@april.com>
Date: Friday, 07/27/04 12:25:31 PM EDT
URL: tylaska@comcast.com

Here are some possible ideas for April Fool's spoof products. Also did some research on these same ideas at the usual site.

In thinking of these ideas I tried to keep in mind the following (perhaps obvious) tenets:

Purpose of the April Fool's Prank:

1. Cause maximum confusion
a. Not from people who know spoof products are fake, but from those who don't
b. Not from media who think spoof products are real
2. Support the non-commercialism of the Internet sound
3. April Fool's pranks are not business critical, so spoof products should be non-commercial

Therefore:

1. Spoof products should be commercial, believable
2. The product image/logo should stand out in the crowd

1. Cook Diet

This would play up on the current low-carb diet fad. Instead of a low-carb diet, this diet SHOULD be backed up with some scientific backing. That Therabook is trying to help people lose weight because of possible risks.

- A. All calories count. SCIENCE: If you speed up your metabolism...
- B. Only eat foods that provide cold. SCIENCE: Your body is cold enough, the calories expended to warm the food...
- C. All sugar is bad. SCIENCE: Opposite of the low-carb diet.

2. Remote Controlled Hunger Eliminator

Similar to the Cook Diet idea, but a different angle. A small non-toxic remote is a dial for your hunger level. When you want to be full, stomach. Could be web-enabled to control via a web browser. Web or additional image.

3. The Computer Virus

This will on the per rock top of the PC's. Image could be a cardboard box. Interface allows you to interact with your virus.

Possible funny aspects:

- To keep your virus healthy you feed it a mini ecosystem
- Instead of going to the bathroom, your virus sends spam mail
- Great to help kids learn about technology and the internet
- web version also available

4. Checkmate

Similar to the computer virus, but more complex. Image could be a cardboard box.

Possible foods to include:

- All customized foods
- Matrix version with only red and green pills
- Sushi







USB Waterproof

» **New Industrial Strength**



Evidence

- **Account Activity**
- **Applications**
- **Cell Phone Records**
- **Shipping Records**
- **Credit History**
- **Utility Records**

Resources

- **Preapproved Credit Card Offers**
 - **1-888-5-OPTOUT**
- **DMV can add Fraud Alert**
- **Check with Telephone Company on password**
- **Do Not Call Lists**

Marketing List Opt Out

- **Equifax, Inc.**
Options
PO Box 740123
Atlanta, GA 30374-0123

Experian
Consumer Opt-Out
701 Experian Parkway
Allen, TX 75013

TransUnion
Marketing List Opt Out
PO Box 97328
Jackson, MS 39288-7328

Other Resources

- **FTC**
 - 1-877-IDTHEFT
 - Website <http://www.consumer.gov/idtheft/>
- **FBI**
 - <http://www.ifccfbi.gov/index.asp>
- **SSA**
 - 1-800-269-0271
- **US Postal Service**
- **AG's Office**

- How to use built in firewalls in XP and OS X
<http://security.getnetwise.org/tools/firewall>
- Check your Security Shields Up
<https://www.grc.com/x/ne.dll?bh0bkyd2>
- Good information
<http://www.idtheftcenter.org/index.shtml>
- Junk mail and telemarketers
<http://www.fightidentitytheft.com/junkmail.html>