Avoid ID Theft
How to Deter, Detect, and Defend Against Identity Theft

www.ftc.gov/idtheft
PRESENTATION OVERVIEW

• What is identity theft? How does it happen?
• What can you do? Deter, Detect, Defend
• Data Security
• Computer Security: OnGuardOnline.gov
WHAT IS IDENTITY THEFT?

• It occurs when someone steals your personal information – e.g., credit card or Social Security number – and uses it fraudulently
• It can cost you time and money
• It can destroy your credit and ruin your good name
HOW DOES IDENTITY THEFT HAPPEN?

• Identity thieves may:
  – Go through your trash or “dumpster dive”
  – Steal your wallet or purse
  – Steal your mail or submit a change of address form for your mail
  – Use “phishing” or fake emails to get you to provide personal information
  – Steal personnel records from their employers
RISKS FOR STUDENTS

- 1/3 IDT victims reporting to FTC in 2005 under 30 years old
- RISKS:
  - Dormitory burglaries
  - Driver’s license/student ID theft
  - Credit card offers
  - Use of Social Security numbers for identification
Recent Surveys on IDT

• 2003 FTC Survey
  – 9.9 million victims in the past year
  – Cost to Business $51.4 Billion (inflation adj)
  – Cost per incident to consumer $4800

• 2006 Javelin Survey
  – 8.9 million victims in the past year
  – Cost to Business more than $50 Billion
  – Cost per incident to consumer $6383
Who’s being me?

- 26% know who stole their identity. Of this:
  - 26% are family members
  - 18% a “friend”, neighbor or in-home employee
  - 13% employee at a financial institution
WHAT CAN YOU DO?

• DETER
  – Deter identity thieves by safeguarding your information

• DETECT
  – Detect suspicious activity by routinely monitoring your financial accounts and billing statements

• DEFEND
  – Defend against identity theft as soon as you suspect a problem
• DETER identity thieves by safeguarding your information.
  – Shred financial documents before discarding them
  – Protect your Social Security number
  – Don’t give out personal information unless you’re sure who you’re dealing with
  – Don’t use obvious passwords
  – Keep your information secure
• DETECT suspicious activity by routinely monitoring your financial accounts and billing statements.
  – Be alert
    • Mail or bills that don’t arrive
    • Denials of credit for no reason
  – Inspect your credit report
    • Law entitles you to one free report a year from each nationwide credit reporting agencies if you ask for it
    • Online: www.AnnualCreditReport.com;
    • By phone: 1-877-322-8228; or by mail
  – Inspect your financial statements
    • Look for charges you didn’t make
DEFEND

DEFEND against identity theft as soon as you suspect a problem.

– Place a “Fraud Alert” on your credit reports by calling any one of the three nationwide credit reporting companies:
  • Equifax: 1-800-525-6285
  • Experian: 1-888-397-3742
  • TransUnion: 1-800-680-7289
– Review reports carefully, looking for fraudulent activity
– Close accounts that have been tampered
– File a police report
– Contact the Federal Trade Commission
ID THEFT EDUCATION KIT

- FTC Tools for educating your community are available from UC InfoSec
  - Talking About Identity Theft: A How-To Guide
  - “Avoid ID Theft” brochure – easy to reproduce
  - PowerPoint presentation
  - 10-minute video (Watch at ftc.gov/idtheft)
Things to Consider ...for UC

• Are staff and faculty sensitive to security/privacy issues?
• Are they alert to social engineering?
• Who has access to employee/student records?
• Are background checks needed?
• How is access restricted?
...for Information Systems

- Appropriate security and firewall protection
- Password protocols - encryption
- Storage and disposal of hard drives
- Rules for laptops
- Wireless concerns
...for Low Tech Issues

- Disposal of records – credit reports
- Delivery of mail – access to mail boxes
- TELLING SOMEONE
Who’s Minding the Data?

- BJ’s Wholesale Club - $15 million in losses
- ChoicePoint – 145,000+ identities
- Card Systems – Tens of millions of card holders
- DSW – 1.5 million customers
- Nations Title – Loan applications in the dumpster
- 9/22/2006 - The Commerce Department reported 1,137 of its notebook computers as lost, stolen or missing since 2001, with 249 of them containing personally identifiable information. Each laptop contained census data from 30 to 100 households.
First Steps Following a Breach

• Assess the situation
• Notify
  – Law Enforcement
  – Those whose information was compromised
  – Early notification allows them to take measures to minimize risk
  – Affected institutions, e.g. banks and card issuers
• Go to “Information Compromise”
  ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm
Seven Practices for Safe Computing – 1

• Protect your personal information: It’s valuable
  – Ask questions
  – Don’t click on the link
Seven Practices for Safe Computing – 2

• Know who you’re dealing with
  – Research sellers, or sites offering free software
  – Check the physical address and phone number
Seven Practices for Safe Computing – 3

• Use **all** of these:
  – anti-virus software
  – anti-spyware software
  – firewall

• Get yours free from UCIT
  [http://www.uc.edu/ucit/ware/software/mcafee.html](http://www.uc.edu/ucit/ware/software/mcafee.html)

• Update regularly (or automatically)
Set up your OS and browser correctly

- Choose appropriate security settings
- Update regularly
Seven Practices for Safe Computing – 5

- Protect your passwords
  - Keep passwords in a secure place
  - Don’t share on the Internet, over email, or on the phone
  - Longer is better
  - Check out the OIS Site for Tips!
    [http://www.uc.edu/infosec/password/choosepassword.htm](http://www.uc.edu/infosec/password/choosepassword.htm)
Seven Practices for Safe Computing – 6

- Back up important files
  - Copy files onto a removable disc or drive
  - Store in a safe place
Seven Practices for Safe Computing – 7

- Learn who to contact if you have a problem
  - abuse@uc.edu
  - OnGuardOnline.gov/fileacomplaint.html has information on how to report different problems
  - Send spam to spam@uce.gov
WHERE CAN YOU LEARN MORE?

• From UC Information Security
  – www.uc.edu/infosec/
    • How To… Fight Identity Theft

• infosec@uc.edu
WHERE CAN YOU LEARN MORE?

- From the Federal Trade Commission
- Online: ftc.gov/idtheft
- By phone: 1-877-ID-THEFT
- By mail: Identity Theft Clearinghouse
  Federal Trade Commission
  600 Pennsylvania Avenue, NW
  Washington, DC 20580
WHERE CAN YOU LEARN MORE?

• OnGuardOnline.gov
  – Internet fraud
  – Computer security
  – Online privacy
• Partners: government agencies, tech industry, non-profits
• In Spanish: AlertaEnLinea.gov
ABOUT ONGUARD ONLINE

• A variety of compelling materials
  – Articles
  – Videos
  – Tutorials
  – Interactivity

• Practical, plain-language tips
  – Hackers, viruses, scams, ID theft
  – Spam, phishing, spyware
  – P2P, social networking
Wrap Up

• Materials are free and available – please use them to educate your communities

• Contact the UCIT Office of Information Security: infosec@uc.edu