PREVENTING IDENTITY THEFT
AT
The University of North Carolina
at Greensboro

Presented By
Roy Davenport
Shred-it North Carolina
Identity Theft in the US: How **BIG** Is The Problem?

- FTC Says it is the fastest growing consumer crime in the country.
  Javelin Strategy and Research report:
  - 13 million victims of identity theft in 2007
  - Nearly 1,000,000 new victims a month
    - New victim every 79 seconds
  - Annual fraud cost of $56 billion
Identity Theft in the US - Now #1 Consumer Complaint

In the U.S. Identity theft made up 39% of consumer complaints to FTC but in N.C. they accounted for 67% of all consumer fraud complaints
Last Year in North Carolina how many citizens became Victims of Identity Theft ???

300,000

That’s nearly 4% of the population
WHAT ARE THE REASONS FOR THIS SKYROCKETING CRIME RATE?

FTC Consumer Complaints (National)

Thousands

<table>
<thead>
<tr>
<th>Year</th>
<th>ID Theft</th>
<th>All Other Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Relatively Easy to Commit.

- Many businesses and individuals don’t have secure ways to store and dispose of confidential information.
- Many still put confidential information in the trash.
- Many place outgoing mail in their mailbox and raise the red flag.
- Many persons do not routinely check credit reports.
- Many do not have adequate computer security.
- Many are too careless about sharing confidential information via the Internet or over the phone.
Hard to Catch and Convict.

- Many victims never know how or when their information was stolen.
- Differences in laws and jurisdictions make convictions difficult.
- Many companies would rather just close an affected account than go to the expense of prosecution.
- Identity Thieves don’t even have to be in the same country to steal your Identity.
Rewards Outweigh The Risks

- Identity Thieves can run up tens of thousands of dollars in debt in your name.
- If caught they sometimes face light sentences or even probation.
- Identity Theft is often seen as white collar crime and victimless.
Pretty Good Odds!

- Rob a bank and there’s a 97% chance you will be caught and prosecuted.
- Steal someone’s Identity and there’s only a 2% chance of ever being caught and convicted!
- That means Identity thieves have a 98% chance of stealing your Identity and getting away with it.
# How Information is Obtained

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost/stolen wallet/credit card</td>
<td>30</td>
</tr>
<tr>
<td>Friend/relative with access</td>
<td>15</td>
</tr>
<tr>
<td>Corrupt employee</td>
<td>10</td>
</tr>
<tr>
<td>Accessed during transaction</td>
<td>10</td>
</tr>
<tr>
<td>Stolen mail</td>
<td>5</td>
</tr>
<tr>
<td>Dumpster Diver</td>
<td>5</td>
</tr>
<tr>
<td>Spyware</td>
<td>5</td>
</tr>
<tr>
<td>Online transaction access</td>
<td>5</td>
</tr>
<tr>
<td>Hacker/virus</td>
<td>5</td>
</tr>
<tr>
<td>Email posing as legitimate business</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Lost/stolen wallet/credit card**: 30%
- **Friend/relative with access**: 15%
- **Corrupt employee**: 10%
- **Accessed during transaction**: 10%
- **Stolen mail**: 5%
- **Dumpster Diver**: 5%
- **Spyware**: 5%
- **Online transaction access**: 5%
- **Hacker/virus**: 5%
- **Email posing as legitimate business**: 5%
How Information is Used

- Credit Card Fraud: 28%
- Phone/Utilities Fraud: 19%
- Bank Fraud: 18%
- Employment-Related Fraud: 13%
- Loan Fraud: 5%
- Other: 22%
Recovery is Expensive!

- Most victims of Identity Theft can expect to spend as many as 800 man hours trying to restore their credit and reputation.
- It can cost as much as $10,000 out of pocket expense.
- Some victims NEVER recover financially!
Colleges and Universities Are Prime Targets for Identity Thieves
Why?

- Large volume of documents and data in one location.
- So many persons living and working in close proximity to each other?
- Financially inexperienced students present opportunities for ID theft.
- Inadequate security of documents and data.
- Many older documents still contain SSN
- Nearly 50% of Universities still use SSN as student identifier.
Some Statistics To Ponder…

• According to the FTC, college students and young adults age 19-29 are more likely to be targeted than any other age group.
• 29% of all FTC complaints of ID theft in 2007 were in this age group.
• 49% of college students receive credit card offers on a weekly basis.
• 30% throw those offers in the trash without destroying them first.
• Nearly 30% of students rarely or never balance their check books.
A Few Data Breaches at U.S Universities in 2008

- New Mexico State U. - Hard drive containing names and SSN of thousands of current and former employees stolen.
- University of Georgia - Foreign hacker breaches housing computer-4250 records accessed.
- Georgetown U. - Hard drive stolen from Office of Student Affairs-38,000 records stolen.

*Privacy Rights Clearinghouse Report May, 2008
High Profile Data Breaches*  
(2005-2008)

- George Mason U. 32,000
- U. of Colorado- 30,000
- U. of CA. Berkely-98,400
- Boston U.- 120,000
- Tufts U.- 106,000
- Duke U. 5,500
- U.S.C- (Columbia) 1,400
- U. of Hawaii- 150,000
- U. of Texas- 197,000
- Valdosta State- 40,000
- Michigan State- 40,000
- U.S.C.- 270,000
- Ohio U. 362,000
- Ga. Southern- 30,000
- E. Carolina U. 250
- Purdue U.- 11,360
- U. of Alaska- 38,900
- U. of Las Vegas- 5,000
- Ca. State U.- 59,000
- U. Of N. Colorado- 30,000
- OK State U. - 37,000
- U. of CA-SF- 7,000
- U. of CO. Boulder- 49,000

*Privacy Rights Clearinghouse  
Report May, 2008
How Information is Accessed

- Hackers breach security to servers.
- Personal laptops stolen.
- Computer media stolen
- Unauthorized access to computers.
- Theft of junk mail/credit card offers
- Unauthorized access of documents.
- Dumpster Diving
- Theft of purses/wallets
What Can Universities Do?

- Identify what confidential information you collect and maintain.
- Identify and understand which laws apply to you.
- Determine who has access to them (staff, non-staff).
- Have a secure way to store and destroy documents for staff and employees.
MORE THINGS UNIVERSITIES CAN DO....

• Use randomly generated ID numbers instead of SSN.
• Train faculty, staff and students on ways to protect their identity.
• Limit access to confidential information by temporary employees or student employees.
• Have up-to-date security for computers and networks.
• Keep an up-to-date written information management policy for the university.
• Train faculty and staff on policies and procedures.
Who is Protecting Us?

- Legislation to safeguard information:
  - FACTA
  - HIPAA
  - GLB Act
  - N.C. Identity Theft Law

Until recently ID Theft was not illegal in some states.
FACTA
(Fair and Accurate Credit Transactions Act)

- Affects businesses who access consumer information and have as few as 100 transactions a year.

- Requires affected businesses to have written policies in place for handling consumer information.

- Who, What, When, Where, How

- “Disposal Rule” specifies proper records destruction such as shredding

- Civil liabilities for willful non-compliance

- Employers, landlords, mortgage companies, auto dealers, insurers etc.
Health Insurance Portability and Accountability Act

Requires:

• Improved efficiency in healthcare delivery by standardizing electronic data interchange.

• Protection of confidentiality and security of health data through setting and enforcing standards.

• More specifically, HIPAA called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure:

  • Standardization of electronic patient health, administrative and financial data
  • Unique health identifiers for individuals, employers, health plans and health care providers
  • Security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present or future.
Health Insurance Portability and Accountability Act

Who’s Affected?

• All healthcare organizations
• Life insurers
• Information systems vendors
• Universities

Penalties?

• Fines up to $25K for multiple violations of the same standard in a calendar year
• Fines of up to $250K and/or imprisonment up to 10 years for knowingly misusing individually identifiable health information
The Gramm-Leach Bliley Act
The Financial Modernization Act of 1999

- Includes provisions to protect consumers’ personal financial information held by financial institutions.
- The GLB Act gives authority to federal agencies and the states to administer and enforce the:
  - Financial Privacy Rule
  - Safeguards Rule
North Carolina Identity Theft Law

- Allows consumers to place “Freeze” on release of their credit report.
- Requires businesses in N.C. or who do business in N.C. to take reasonable precautions to protect personal information.
- Limits use of SSN over Internet and mail
Things Each of Us Can Do?

• Never keep SS card in your wallet/purse.
• Limit the number of credit cards you carry.
• Limit use of your Social Security Number.
• Maintain inventory of account numbers.
• Don’t give out personal information unless you know who you’re giving it to.
• Ask about employers’ privacy policies.
• Never place confidential information in your mailbox.
• Never, ever place confidential information in the trash…..shred before disposing!
More Things We Can Do...

• Periodically check your credit report.
• Make sure your computer has up to date virus and spy ware protection.
• If you provide confidential information via the Internet make sure the site is secure. Look for a “lock” symbol or URL that begins with “https”:
• When you dispose of old computer make sure you use a “Wipe” program to securely erase data on your hard drive.
• Use a personal firewall if you have high speed Internet connection that leaves your computer connected at all times.
How To Know If You’re A Victim

• Failure to receive your mail
• Receiving credit cards you did not apply for.
• Denial of credit for no apparent reason.
• Receiving calls from debt collectors or companies about charges you didn’t make.
• Charges on your credit card bill that you didn’t make.
What To Do If You Become a Victim!

1. Immediately place a Fraud Alert on your credit reports by contacting one of the three reporting agencies. (Equifax, Transunion, Experian)

2. Order copies of credit reports from all three agencies and review them carefully.

3. Contact and close all affected accounts.

4. Report your case to FTC.

5. Report your case to local Police.
Resources

www.ftc.gov

www.ncsl.org/programs/lis/privacy/idt-statutes.htm

www.fightidentitytheft.com

www.shreedit.com
THANK YOU!

QUESTIONS?