Identity Theft
Help Your Students Avoid This Epidemic – Sun Ow
34% of identity theft victims are college students
Did You Know...

• Only 24% of fraudulent charges were first caught by a consumer’s financial institution
• Every three seconds someone's identity is stolen
• The FTC estimates that as many as 9 million Americans have their identities stolen each year
Why College Students May Become a Target

- Moving to campus locations and living with roommates
- Placing orders over the internet in public places
- Discarding credit card offers without shredding them
Why College Students May Become a Target

- Being careless with student IDs, PINs, and credit card information
- Using cell phones in public and divulging sensitive information
- Leaving dorm rooms unlocked
- Walking away from laptops or tablets
Objectives

1. Recognize the types of identity theft
2. Discuss ways in which identity theft occurs
3. Review the potential impact
4. Identify ways to protect themselves
Objectives

5. Determine what to do if they suspect a problem

6. Pinpoint techniques to prevent being a victim

7. Share ways to educate your students
## Test Your “Identity IQ”

<table>
<thead>
<tr>
<th>Statement</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>One out of four people are affected by identity theft</td>
<td>True</td>
</tr>
<tr>
<td>Identity theft issues are resolved quickly once reported to the authorities</td>
<td>False</td>
</tr>
</tbody>
</table>
# Test Your “Identity IQ”

<table>
<thead>
<tr>
<th>Statement</th>
<th>True/False</th>
</tr>
</thead>
<tbody>
<tr>
<td>7% of all adults have their identities stolen from gov’t or corporate databases</td>
<td>True</td>
</tr>
<tr>
<td>Identity theft is not a serious crime</td>
<td>False</td>
</tr>
<tr>
<td>College students comprise the single largest demographic of all identity theft victims</td>
<td>True</td>
</tr>
</tbody>
</table>
What Are the Types of Identity Theft?
First: What Is It?

- Identity theft occurs when an unauthorized person steals your personal information and uses it to commit identity fraud by
  - Opening credit accounts
  - Obtaining a job
  - Getting a loan
  - Committing a crime
  - Using an existing account
Second: What’s the Harm?

- Identity theft can ruin your credit
- Recovering your credit and your good name can be time consuming and expensive
Types of Identity Theft

1. Financial identity theft
2. Criminal identity theft
3. Identity cloning
4. Business/commercial identity theft
# Consumer Sentinel Network

## Identity Theft Complaints by Victims’ Ages

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 and Under</td>
<td>7%</td>
</tr>
<tr>
<td>20 - 29</td>
<td>24%</td>
</tr>
<tr>
<td>30 - 39</td>
<td>22%</td>
</tr>
<tr>
<td>40 - 49</td>
<td>19%</td>
</tr>
<tr>
<td>50 - 59</td>
<td>15%</td>
</tr>
<tr>
<td>60 - 69</td>
<td>8%</td>
</tr>
<tr>
<td>70 And Over</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: Consumer Sentinel Network
How Does Identity Theft Occur?
<table>
<thead>
<tr>
<th></th>
<th>False identification</th>
<th></th>
<th>Social engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Credit card fraud</td>
<td>5</td>
<td>Dumpster diving</td>
</tr>
<tr>
<td>3</td>
<td>Computer hacking</td>
<td>6</td>
<td>Mail theft</td>
</tr>
</tbody>
</table>
The Thief in the Machine

- **Skimming**
  - Captures information on a data storage device

- **Phishing**
  - Captures information through email or phone

- **Pharming**
  - Captures information through a fake website
The Thief in the Machine

- **Vishing**
  - A form of phishing that is short for voice-phishing
  - Captures information using VoIP (Voice over Internet Protocol)
  - Accomplished through emails or cold calls
Social Media Statistics: By-the-Numbers

15% of Americans have never checked their social networking privacy and security account settings.

25% of teen Facebook users share photos and videos of themselves and tag friends.

National Cyber Security Alliance (NCSA)-MacAfee Online Safety Study, 2011
PEW Research Center, 2013
Social Media Statistics: By-the-Numbers

23% of teen profile creators say it would be "pretty easy" for someone to find out who they are from the information posted on their profile.

21% of teen Facebook users share their personal cell phone number.

InternetSafety101.org
PEW Research Center, 2013
Did You Know...

- 25% of Facebook users don’t bother with privacy settings
- Facebook users share 2.5 billion pieces of content per day
- 40 million photos are posted in Instagram a day
- Flickr hosts more than 4 billion images
Did You Know...

- 72% of teens have a social networking profile and nearly half (47%) have a public profile viewable by anyone.
- Of the active adult users of Facebook, 66% reported they did not know privacy controls existed on Facebook and/or they did not know how to use them.

Internetsafety101.org
Consumer Reports, June 2011
Did You Know...

- 76% of teens are at least somewhat concerned that posting information publicly could negatively impact future
- 26% of teens know someone something bad has happened to because of information or photos posted online
- 36% of 18-29 year olds have and use Instagram regularly

Internetsafety101.org
“Friends” May Not Be Friends

Social networks can be a target of identity theft

It’s important to:

– Use anti-phishing filters
– Use the official networking site
– Be suspicious of anyone who asks for money
“Friends” May Not Be Friends

It’s important to:

– Verify circumstances independently, preferably by direct telephone contact
– Use different passwords for all web accounts
– Include more than one contact email address
– Review a site’s security page for
  • Current alerts
  • Steps to take if you become a victim
Students Put Themselves at Risk

- Tweeting that they’re enjoying some alone time
- Facebook status updated that they’re away from home or out-of-town
- Including personal statistics such as birth date, address, cell phone number
- Accepting “friend” requests from people they do not know
Other Methods of Identity Theft

- Identity thieves steal information from:
  - Personnel records from employers
  - Mailboxes (or by redirecting mail with a change of address form)
  - Personal belongings from someone’s home
  - Wallets or purses
  - Databases
What is the Impact?
Students May be Unaware

• Young people are easy targets
• Identity theft among young people:
  – Remains undetected, sometimes for years
  – Is stolen at more than 50 times the rate of adults
  – Shows no obvious warning signs
  – Is easier to rectify than with an adult case

Source: Reuters, July 11, 2011
It’s Not Always Random

Information can be stolen by:

- Relatives
- Doctor’s offices
- Friends
- Schools
- Hospitals
Financial Aid Victims of Identity Theft

- A victim of IRS identity theft who is not able to obtain an IRS Tax Return Transcript or use the IRS Data Retrieval Tool (DRT) must contact the IRS at 1-800-908-4490.
- Upon authentication of the tax filer’s identity, the IRS will provide, by U.S. Postal Service, a printout of the tax filer’s IRS income tax return information which can be used to complete verification.
How Can Students Protect Themselves?
The Three Ds of Identity Theft

DETER, DETECT, DEFEND

Deter identity thieves by safeguarding your information
Detect suspicious activity by monitoring statements and accounts
Defend against identify theft as soon as you suspect a problem
Don’t Give Thieves the Red Flag

• Send important mail from the post office or a USPS mailbox—not your home mailbox
• Use a locked mailbox
• Stop mail/newspapers when on vacation
• Request special delivery for check orders
• Opt out of pre-approved credit card offers
  – optoutprescreen.com or 1-888-567-8688
Hang onto Purses and Wallets

• Keep your purses and/or wallets in a secure location
• Don’t keep seldom used credit cards in your wallet
• Don’t carry your checkbook if you don’t plan to use it
• Keep your Social Security card and/or passport in a safe place
Remain Cautious

• Don’t think that “See I.D.” will stop criminals from using a stolen card
• Use caution with financial aid forms, documents, and other materials with personal information
  – Students should consider having a locked file cabinet or safe
Use Online Precautions

• Use strong passwords and change them often
  – howsecureismypassword.net

• Don’t give out sensitive information
  – SSN
  – Date of birth
  – Bank account information, etc.
Use Online Precautions

• Use secure websites
• Don’t open email from strangers
• Use a firewall
• Update virus software regularly
Use Online Precautions

• Use the highest level security setting
• Read privacy and security policies
• Use the least amount of personal information possible

Idtheftcenter.org
Use Online Precautions

• Be wise about your online postings
• Connect only to those you know
• Watch emails and links

ldtheftcenter.org
Be on the Lookout for Suspicious Activity

• Unexpected credit denials
• Unexpected charges on monthly financial statements
• Unexpected credit card approvals
• Calls or letters from debt collectors
Be on the Lookout for Suspicious Activity

• Protect personal data
  – Shred documents
  – Don’t share too much information on social networks

• Monitor bank and credit accounts

• Pay attention to official notices
Monitor Your Credit Report

• Get a free credit report every year
  – annualcreditreport.com
  – (877) 322-8228

• Review credit card offers, then shred
What Can Students Do if They Suspect a Problem?
If They Have Been Victimized

They should:

– Close their accounts
– File a detailed police report
– Place a fraud alert on their credit reports

Equifax: (800) 525-6285
Experian: (888) 397-3742
TransUnion: (800) 680-7289
## Identity Theft Complaints

File a complaint with the Federal Trade Commission

<table>
<thead>
<tr>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>ftc.gov/idtheft or <a href="https://www.consumer.ftc.gov/features/feature-0014-identity-theft">https://www.consumer.ftc.gov/features/feature-0014-identity-theft</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(877) ID-THEFT</td>
</tr>
<tr>
<td>Mail</td>
<td>Identity Theft Clearinghouse Federal Trade Commissions 600 Pennsylvania Ave. NW Washington, DC 20580</td>
</tr>
</tbody>
</table>
Identity Theft Complaints

• Create an identity theft report
  – Use an identity theft complaint form, which entitles students to certain protections, along with a police report
Identity Theft Report

• Students can use an Identity Theft Report to:
  – Permanently block fraudulent information from appearing on their credit report
  – Ensure that debts do not reappear on their credit report
  – Prevent a company from continuing to collect debts that result from identity theft
  – Place a fraud alert protection on their credit report
Fraud Alert Protection

• Initial Alert
  – Stays on a student’s credit report for at least 90 days
  – Entitles them to one free credit report from each credit reporting agency
  – Lists only the last four digits of their SSN
Fraud Alert Protection

• Extended Alert
  – Stays on a credit report for seven years
  – Requires an identity theft report
  – Entitles students to two free credit reports per year
  – Removes their name from marketing lists for five years
Fraud Alert Protection

• Extended Alert
  – Ensures that businesses contact them directly before issuing credit
  – Requires proof of their identity to place and/or remove an alert from their credit report
Are There Ways to Be Proactive?
Proactive Measures

- Insurance
- Credit Monitoring
- Credit Freeze
- Self-Monitoring
- Fraud Alert
Identity Theft Insurance

• Coverage can be in many ways
  – Separate policy
  – Part of existing insurance policy
  – Through credit card company
  – Included in credit monitoring

• Think about the types of losses and coverage available after the deductible
Credit Monitoring

• Many companies from which to choose
• Multiple types of monitoring available
  – Credit reports
  – Public records
  – Credit cards
  – Social security
• Fees range from $5 - $17 per month
Credit Monitoring

• Provides updates to customers including information about credit checks and new accounts
• Receive immediate notification about any suspicious activity on their credit report
• Many offer different levels of service for varied fees
Fraud Alert

• Requires credit reporting agencies to use "reasonable policies and procedures" to verify your identity before opening an account

• Only need to set it with one credit agency and they will report it to the others
Credit Freeze

• Stops access to a student’s credit report file
  – Prevents fraudulent opening of new accounts in their name

• Credit freeze laws exists in most states
  – Voluntary programs are available from the three major credit reporting agencies
Credit Freeze

- Consumer has more control of access to credit file
  - PIN provided
- Does not affect existing accounts
  - Does not stop misuse of existing accounts
Self-Monitoring

Proactive safekeeping of personal information is the most effective—and it’s free
What Can You Do to Educate Your Students?
Ways You Can Help Your Students

1. Recommend they have a shredder

2. Reinforce the importance of providing information only on secure websites

3. Explain how to monitor their credit report

4. Caution them about what they share on social media
Ways You Can Help Your Students

5. Remind them to have spyware and an anti-virus program installed on their notebook or PC

6. Encourage students to avoid accepting requests to interlink their Facebook and other social media accounts with people they don't know

7. Provide them with resources
Helpful Resources

Credit Reporting Agencies

– Experian.com
– Equifax.com
– Transunion.com

Privacyrights.org (Privacy Rights Clearinghouse)

Identitytheft.gov and Fraud.org (National Fraud Information Center)
<table>
<thead>
<tr>
<th>Helpful Resources</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>fcc.gov and ftc.gov</td>
<td>idtheftcenter.org</td>
</tr>
<tr>
<td>sec.gov</td>
<td>ncvc.org</td>
</tr>
<tr>
<td>ed.gov/misused</td>
<td>epic.org</td>
</tr>
</tbody>
</table>
Thanks for Attending

Contact Information: Sun Ow
Senior Marketing Associate
(866) 348-0710
sow@glhec.org