Armstrong State University
Fall Staff Assembly

IDENTITY THEFT IS ON THE RISE
WHAT YOU NEED TO KNOW

Chief Wayne Willcox, MSCJ, CLEE
Identity Theft:
• When someone uses your personal information without your permission to commit fraud or other crime
  – Name
  – Social Security number
  – Date of birth
  – Credit card number
  – Bank account numbers
Why Be Concerned?

MEMO TO SELF: IDENTITY THEFT PROBLEM GETTING WAY OUT OF HAND.
In 2014:

- 12.7 Million Americans Became Victims
- $16,000,000,000 in Losses
In 2014:

- New Victim every 2 seconds
4 Biggest Targets:

1. People age 18-24
   29%

2. Those making more than $75,000
   10%

3. People with weak passwords

4. Young children
   150,000 annually
## Types of Fraud

<table>
<thead>
<tr>
<th>Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit card</td>
<td>25%</td>
</tr>
<tr>
<td>Phone/utilities</td>
<td>16%</td>
</tr>
<tr>
<td>Bank account</td>
<td>16%</td>
</tr>
<tr>
<td>Employment-related</td>
<td>14%</td>
</tr>
<tr>
<td>Fraudulent tax return</td>
<td>6%</td>
</tr>
<tr>
<td>Business/personal/student loan</td>
<td>3%</td>
</tr>
</tbody>
</table>
## Types of Fraud

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet/email</td>
<td>2%</td>
</tr>
<tr>
<td>Medical</td>
<td>2%</td>
</tr>
<tr>
<td>Auto loan</td>
<td>2%</td>
</tr>
<tr>
<td>Driver’s license</td>
<td>1%</td>
</tr>
<tr>
<td>Real estate loan</td>
<td>1%</td>
</tr>
<tr>
<td>Gov’t benefits</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>24%</td>
</tr>
</tbody>
</table>
How does Identity Theft occur?
Good, Old Fashioned Stealing
New NFC Contactless Tag Reader Writer Magnetic Card Reader For Smart Phones FS

Item condition: New

Quantity: 1 More than 10 available

Price: US $49.90

Buy It Now
Add to cart

Free shipping Expienced seller New condition

Shipping: FREE Economy Shipping from outside US | See details

Seller information
finetech007 (58244/5*)
99.2% Positive feedback

Follow this seller
Visit store: finetech007
See other items

Back to search results | Listed in category: Business & Industrial > Retail & Services > Point of Sale Equipment > Credit Card Terminals, Readers
Dumpster Diving
Dear Wachovia Bank customer,

Wachovia is pleased to notify our online banking customers that we have successfully upgraded to a more secure and encrypted SSL servers to serve our esteemed customers for a better and more efficient banking services in the year 2007.

Due to this recent upgrade you are requested to upgrade your account information by following the reference below, using our new secure and safe SSL servers.

To validate your online banking account click on the following link:
https://onlineservices.wachovia.com/auth/AuthService?action=presentLogin

This email has being send to all our bank customers, and it is compulsory to follow as failure to verify account details will lead to account suspension.

Thank you,
Wachovia Online Banking Security Team.

© 2007 Wachovia Corporation. All rights reserved.

Dear Bank of America Member,

We are contacting you regarding your Bank of America online account. Due to incorrect information provided during your signup process, your account has been deactivated.

Therefore we invite you to update your profile in order to regain full access to our services.

CLICK HERE TO UPDATE

Please Note: If your account information is not updated within next 24 hours, your account will be suspended.

We apologize for any inconvenience this may have caused.

Sincerely,
Bank of America Customer Care

http://boaupdate.pochta.ru (RUSSIA)
PHISHING

Emails that appear to be from IRS requesting you confirm information.

Emails that are thanking you for a recent purchase (of something you didn’t buy)

Phone phishing

When in doubt, ask or “call back”
Your bank will NEVER ask you for account numbers or passwords if they initiated the communication
How do you prevent Identity Theft?

1. Consider subscribing to an identity theft protection service.

BUT !!!!

1. Expensive
2. Biggest burden is time, not money
How do you prevent Identify Theft?

2. Keep personal documents in a safe. Consider keeping a personal safe for your home as well as a safety deposit box elsewhere. You can use your safe at home to protect items such as your social security card, birth certificate and passport.
How do you prevent Identify Theft?

3. Protect your purse or wallet at all times. The best purses are those that can be zipped or closed shut. Try not to use bags that others can easily see or reach into, and keep bags close to your body with a tight grip at all times. Do not leave wallets or purses in the car, or if you must, do not leave them exposed or in an obvious place.
How do you prevent Identity Theft?

4. Photocopy the contents of your wallet. Make copies of credit cards, ID cards, and all other personal documents you keep in your wallet. Also, keep records of phone numbers to contact in case you need to close accounts or order replacement items. ( encrypt & export keys & EFS Certificate )
How do you prevent Identify Theft?

5. Examine your bank account statements monthly to ensure that your accounts have no unauthorized charges. If they do, contact your banking institution immediately.
How do you prevent Identity Theft?

6. Remove yourself from promotional lists such as junk mail and pre-approved credit card lists. This added clutter doesn’t do any good, and you at risk of ID theft if a stranger gets their hands on your pre-approved cards.
How do you prevent Identify Theft?

7. Cancel credit cards that you aren’t using. There’s no reason to have open credit for the taking. Besides, the less credit you have open, the less you’ll have to monitor.
How do you prevent Identity Theft?

8. Select passwords that are difficult for others to uncover. An impersonal combination of letters and numbers is the best.

Most frequently used Passwords
1. 123456
2. password
3. 12345
How do you prevent Identify Theft?

9. Protect your computer with anti-spyware and anti-virus software. Make sure you keep them up to date.

Is your firewall on?
How do you prevent Identify Theft?

10. Do not reveal personal information to unverified sources whether over the phone or the Internet. Do not feel pressured to answer personal questions if you do not trust the source. Feel free to request verifying information before giving anything up.
How do you prevent Identify Theft?

11. Monitor your credit. Take advantage of your free credit reports and consider purchasing additional copies throughout the year for continuous monitoring. Consider placing fraud alerts and credit freezes on your account for greater protection.
How do you prevent Identify Theft?

12. Shred personal documents before throwing them away. Dumpster diving is a common method of stealing personal information for the sake of identity fraud. **Purchase a shredder** for your home and make sure you destroy paperwork containing personal information before discarding. This **includes mail, credit card statements and even receipts.**
How do you prevent Identify Theft?

13. Wipe your old computer:


Wiping your phone/tablet:

http://www.cnet.com/how-to/how-to-wipe-your-phone-or-tablet-before-selling/
How do you prevent Identify Theft?

14. Unsecured Wi-Fi

Not a good idea to access sites that require login credentials while on an unsecured wi-fi.

Not good idea to email or message on unsecured wi-fi.

Is your home wi-fi encrypted?
How do you prevent Identify Theft?

15. Always go directly to the company's website rather than clicking on links in the emails (PHISHING)
How do you prevent Identify Theft?

16. Online Purchases & Online Banking/Bill Payment

Safe if you look for https and padlock!

Credit cards Vs Debit and Check #

Do not click on pop-up ads when on retail site
5. Georgia

- Identity theft complaints per 100,000: 112.7
- Total complaints per 100,000 population: 777.7 (2nd highest)
- Total complaints: 78,526 (5th highest)
- Average amount paid: $1,750 (16th lowest)

False Tax returns with stolen Social Security numbers
Strengthening Your Digital Security

Don't use the same password for all of your accounts. Vary the passwords from account to account. Avoid easily guessed PINs like birth dates, common numerical sequences, phone number, the last four digits of your social security number, etc.

Good passwords will include capital and small letters, numbers and characters, and be at least 8 characters long. Never store passwords or sensitive information on your computer. All computers are hackable. If you need to keep this information digitally, store it on a CD or in an external hard drive that is only attached to the computer for offline backups (turn off your internet connection when making backups).
How secure is your password?

<table>
<thead>
<tr>
<th>Length</th>
<th>Lowercase</th>
<th>+Uppercase</th>
<th>+Nos. &amp; Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 characters</td>
<td>10 minutes</td>
<td>10 hours</td>
<td>18 days</td>
</tr>
<tr>
<td>7 characters</td>
<td>4 hours</td>
<td>23 days</td>
<td>4 years</td>
</tr>
<tr>
<td>8 characters</td>
<td>4 days</td>
<td>3 years</td>
<td>463 years</td>
</tr>
<tr>
<td>9 characters</td>
<td>4 months</td>
<td>178 years</td>
<td>44,530 years</td>
</tr>
</tbody>
</table>
Protect your computer.
Many identity thieves now use complex software such as spyware and keyloggers to obtain sensitive information such as passwords and login details without the user's knowledge.

Just because you can't see anything wrong with your computer doesn't mean that it is safe to use. Unlike viruses and adware, many spyware and keylogger programs are designed for stealth, so that they can gather as many passwords and sensitive data as possible. A strong and regularly updated firewall, anti-virus program and anti-spyware program will provide most of the protection an individual needs.
Beware phishing scams. Phishing involves seemingly harmless emails being sent to you, asking you to verify certain things such as passwords, account numbers or credit/social security details. Any email seeking this sort of information should be an immediate red flag for you. The best response is to contact the service provider directly and ask what's up.
Never answer unsolicited or unwanted emails.

Even if you're joking, the return email verifies your existence to the would-be scammer and it's just better off that they think their attempt to get to you disappeared into the ether.

Avoid opening emails that don't make sense to you or that come from people or organizations that you don't recognize. Viruses or worms can be hidden in emails. Be doubly suspicious if the email ends up in your spam folder. And always have your virus protection updated and turned on.
If someone steals your identity, you have the right to:

• create an identity theft report
• place a 90-day initial fraud alert on your credit report
• place a seven-year extended fraud alert on your credit report
• get free copies of your credit report
• get fraudulent information removed (or “blocked”) from your credit report
• dispute fraudulent or inaccurate information on your credit report
• stop creditors and debt collectors from reporting fraudulent accounts
• get copies of documents related to the identity theft
• stop a debt collector from contacting you.
“Some people call him Santa Claus, some call him Kris Kringle, some call him Saint Nicholas. Obviously, a victim of identity theft!”

Chief Wayne Willcox, MSCJ, CLEE