Seminar Objectives

Learn:

- What identity theft is
- How crooks get your personal information
- When you have to give SSN, and when to say “no”
- How to minimize risk of ID theft—online and offline
- Tips to protect yourself from phishing and pharming attacks
- Warning signs that you may be a victim of ID theft
- What to do if you’re a victim and where to get help
What is identity theft?

It occurs when someone uses your:

- Name
- Social Security number
- Other identifying information

... without your permission, to establish new accounts \textit{in your name}.
How many victims?

- 2007: 8.4 million
- 2006: 8.9 million
- 2005: 9.3 million
- 2003: 10.1 million

*Javelin Strategy and Research, Feb. 2007*

- One in five consumers (19%)

*Experian-Gallup Personal Credit Index, Oct. 2006*

- 15 million Americans victims of ID theft-related fraud in 12 months ending mid-2006

*Gartner Inc., March 2007*
Impact on victims

- Damaged credit record
- Loss of job opportunities
- Refused loans for education, housing, or cars

The average victim …

- Spent 25 hours resolving problems in 2007
- Said the perpetrator got $5,720* in cash, goods, or services in 2007

* Mean fraud amount per fraud victim
Who’s vulnerable? All of us!

Most vulnerable:

- 18- to 24-year-olds
- Urban or suburban households
- Those with incomes > $75,000

(Justice Department, 2006)
How do crooks get your number?

- Lost/stolen wallets
- Misuse by family/friends
- Theft from mailboxes; dumpster diving
- Others (less common):
  - Steal records from employer
  - Shoulder surfing at ATMs or phone booths
  - Pose as landlord to obtain credit report
  - Fill out change of address to divert mail
  - Phishing/pharming
What do crooks do with your personal information?

- Open new accounts in your name and go shopping (Delinquent accounts reported on your credit report)
- Call card issuer and change billing address (Ring up charges before your mail catches up to you)
- Take out loans, buy cars, get phone service in your name
- Authorize electronic transfers to drain your account
- File for bankruptcy in your name to avoid paying debts
- Give your name during an arrest
Variations on an ID theft theme

- Spamming
- Spimming
- Spoofing
- Pretexting
- Keystroke logging
- Skimming
- SMiShing
- Vishing
- Phishing
- Pharming
Beware skimming

- Thief swipes your card through hand-held device or overlay swipe device on ATM

- Device gleans information (name, account number, expiration date, and security features) off magnetic stripe on back of card

- Thief copies security codes from your card to the fraudulent card and sells it to a counterfeiter
What do devices look like?
Another example...

- Front view
- Side view (notice pin hole camera)
A view from the camera...
Beware pretexting

- Crook gets personal information under false pretenses (example: poses as survey firm)
- Pretexters sell information to people who may use it to get credit in your name, steal your assets, or investigate or sue you
- Unlawful to pretext for financial records, as well as for phone records
Spamming, spoofing, and phishing—oh my!

**Spamming**—Sending unsolicited e-mail indiscriminately to multiple mailing lists, individuals, or newsgroups

**Spoofing**—Creating a replica of a legitimate Web page to fool you into submitting personal, financial, or password data

**Phishing**—Luring victims to a fake Web site through spam. See current scams at antiphishing.org

It’s probably a phishing attack!

Beware e-mail messages that:

- Use generic greeting (“Dear Visa customers” or “Dear friend”)
- Refer to urgent problem
- State that your account will be shut down unless you reconfirm billing information
- Urge you to click on link within message you weren’t expecting
Example: IRS Phishing Email

From: Internal Revenue Service [mailto:admin@irs.gov]
Sent: Wednesday, March 01, 2006 12:45 PM
To: john.doe@jdoe.com
Subject: IRS Notification - Please Read This.

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $63.80. Please submit the tax refund request and allow us 6-9 days in order to process it. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here
Regards,
Internal Revenue Service

© Copyright 2006, Internal Revenue Service U.S.A. All rights reserved.
What’s worse than phishing? **Pharming**!

- Practice of redirecting Internet domain name requests to illegitimate Web sites.

- Why? To capture your personal information and commit ID theft.

- Differs from phishing in *how* you’re redirected. Instead of clicking on links within e-mail messages (phishing), pharmers redirect you through technical means.
Pharming can occur four ways …

- **Static domain name spoofing**
  (Misspellings: vvestcu.org vs. westcu.org)

- **Malicious software—Malware**
  (Viruses and Trojans redirect you to the false site)

- **Domain hijacking**
  (Hacker hijacks legitimate site and redirects all traffic)

- **DNS poisoning (most dangerous)**
  (You enter correct URL, but poisoned server redirects)
Take precautions: General tips

- Never give personal information to callers (even IRS).
- Safeguard wallets, purses, checkbooks, and account statements—at home and at work.
- Review statements monthly (more often online).
- Don’t write passwords or PINs on back of card.
- Shred receipts, statements, cancelled checks.
- For online transactions, use Verified by Visa and/or MasterCard’s Secure Code.
Take precautions: Protect your Social Security number

- Ask “Why do you need it?”
- Keep SSN off driver’s license.
- Don’t carry SS card in wallet unless you need it that day.
- Don’t use last 4 digits of SSN as PIN; Memorize PINs!
- Don’t let clerks handwrite SSN on checks as ID.
- Don’t have SSN preprinted on checks (re-order them without SSN).
- Know when you have to give it, and when you don’t.
Know when you **have to** give SSN, and when you **don’t**

**Must give SSN**
- Credit unions/banks
- Employers
- Income tax records
- Loan applications
- Credit bureau reports
- College records

**May want to refuse**
- Over the phone
- On personal checks
- On driver’s license
- On club membership
- As ID for store purchases
- As general identification
Take precautions:
Protect yourself from phishing attacks

- Don’t click on links to Web pages within e-mail messages you weren’t expecting. Contact company directly—call, or retype Web link.
- Look for https:// in the URL.
- Use up-to-date antivirus software and firewall.
- Avoid e-mailing personal and financial information.
- Notify CU or company “spoofed” immediately.

Report suspicious activity to the FTC.
Send spam to spam@uce.gov. File complaints at ftc.gov.
Take precautions: 
Protect your computer

- Install and update current virus protection software
- Install firewall software to partially guard against spyware
- Install spyware detection and removal software
  Spybot Search and Destroy, or Ad-aware
  Beware look-alikes such as No-Adware
- Install a spam blocker, free from antiphishing.org
- Use a secure browser to scramble communications
- Set browser security level to at least medium
  Tools: Macro: Security: Medium
More tips to protect your computer

- Don’t click on links from unfamiliar senders
- Don’t download files or open attachments from strangers
- Use strong passwords—combination of letters (upper and lower case), numbers, and symbols
- Avoid automatic log-in; always log off when done
- Lock computer when you leave the work station
- Lock laptop with security cable; don’t leave it in car
- Don’t use public computers to access accounts
- Securely erase hard drive before disposing of computer:
  - Re-format hard drive, or use hard drive erase utility
Take precautions: *Shop safely online*

- Shop only with companies you know.
- Pay only with credit card, or with third-party intermediary.
- Consider using a separate credit card for online purchases to track purchases easily.
- Use secure browser (look for closed padlock or unbroken key at bottom of browser window—not payment page).
Take action: Be proactive

- Go paperless! Use electronic deposit of paychecks, dividends, pension and SS payments, and tax refunds. Use online bill pay.

- Avoid easily recognizable passwords.

- Keep a list—in a safe place—of account numbers, expiration dates, and numbers to report theft.

- Dry up junk mail:
  -- Get off prescreened credit card lists: 888-5opt-out (optoutprescreen.com)
  -- Register with Direct Marketing Association (MPS) (dmachoice.org/consumerassistance.php)

- Reduce unwanted catalogs (catalogchoice.org).
Take precautions:
Get in the habit ...

- Pick up new checks at credit union.
- Mail bills from locked mailbox or Post Office; Stop mail if you’re out of town.
- Shred (with cross-cut shredder) preapproved credit card offers, statements/bills with account numbers, and other personal documents.
- Guard against shoulder surfers.
- Don’t authorize payment over the phone unless you initiated the call and know the reputation.
- Check your credit report annually, as well as your child’s!
Warning signs you may be a victim of ID theft

- Oftentimes, there aren’t any!
- Your monthly credit card or financial statements contain fraudulent charges or suddenly stop arriving.
- You don’t receive any mail for several days.
- You’re denied credit for no apparent reason.
- You start getting bills from unfamiliar companies.
- Credit collection agencies start calling.
No warning signs?

- Check your credit report anyway!
  - Get one free report per year from each bureau (Annualcreditreport.com)
  - Look for accounts you didn’t authorize
  - Check for accuracy; dispute inaccuracies

- Beware of e-mails and Web sites offering “free” credit reports
  - Don’t give your SSN just to get a free report
If you’re a victim of ID theft …

- Place fraud alert on your credit reports.
- Contact FTC’s ID Theft Hotline at 877-IDTHEFT.
- Close affected accounts. Use FTC’s “ID theft affidavit” at ftc.gov/bcp/edu/microsites/idtheft/.
- Follow each conversation with a certified letter, return receipt requested; keep copies.
- File a police report where ID theft took place.
- Get copies of police reports and send to creditors.
How to order your free credit report

- Get one free report per year from each agency:
  - "annualcreditreport.com, or annualcreditreport.com"
  - Call 877-322-8228, or
  - Send request form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281

- It’s also free if you’re:
  - Denied credit within the past 60 days
  - Victim of identity theft
  - Welfare recipient
  - Unemployed and job-hunting
  - Resident of CO, GA, ME, MD, MA, NJ, and VT
The “big three” credit reporting agencies

Experian
Order report: 888-397-3742
Fraud Unit: 888-397-3742
experian.com

TransUnion
Order report: 800-888-4213
Disputes: 800-916-8800
Fraud Unit: 800-680-7289
transunion.com

Equifax
Order report: 800-685-1111
Fraud Unit: 800-525-6285
equifax.com
More resources ...

OnGuard Online
onguardonline.gov/index.html

Privacy Rights Clearinghouse
privacyrights.org

Anti-Phishing Working Group
antiphishing.org

Consumers Union
consumersunion.org

Download.com

FTC
877-IDTheft
ftc.gov/bcp/edu/microsites/idtheft/

“Big 3” fraud units
Experian 888-397-3742
TransUnion 800-680-7289
Equifax 800-525-6285

Better Business Bureau
bbbonline.org

Internal Revenue Service
irs.gov
800-829-1040

Treasury Inspector General
Fraud Referral Hotline
800-366-4484
Remember … your credit union can help you with all your financial challenges.