

Practicing Safe Text

Protecting your confidential information in a digital age

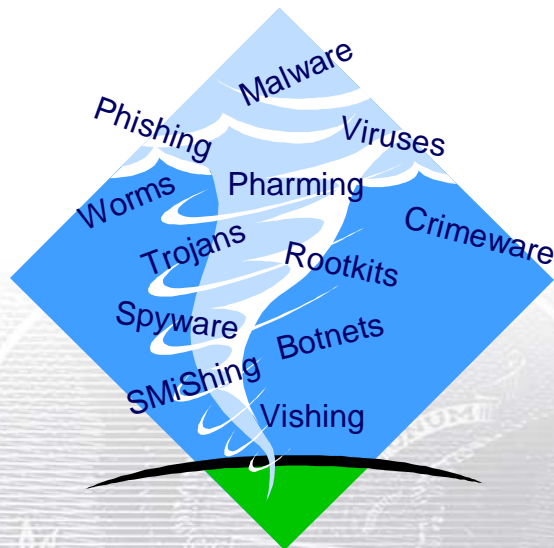
Lynne Pearson, Fifth Third Bank
HFMA Lone Star Chapter Winter Institute
January 21, 2010

Agenda

- Review Identity Fraud Landscape
- Types of Fraud and Their Evolution
- Best Practices in Averting Identity Theft
- What to do if You've Become an Identity Theft Victim
- Identity Fraud Resources
- Wrap up and Questions



Fraud: We're Not in Kansas Anymore



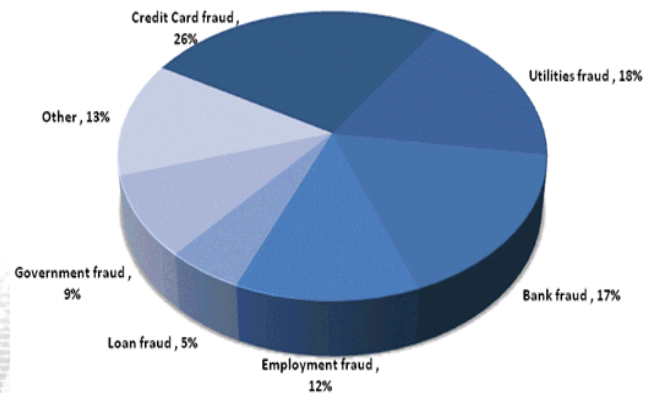
Fraud Continues to Grow

- Over 500 million records have been compromised in the last 5 years containing personal information from government and corporate databases
- Estimates of identity theft now at 10 million victims per year in America
- Less than one-third of victims report crimes to law enforcement and only about 5% report to the FTC (yet identity theft represents 26% of problems reported to the FTC)
- The chances of a criminal being arrested and convicted for identity theft-related fraud are less than 1/2%

Sources: Gartner; FTC, identifytheftinfo.com



Types of Identity Theft Fraud



Source: FTC



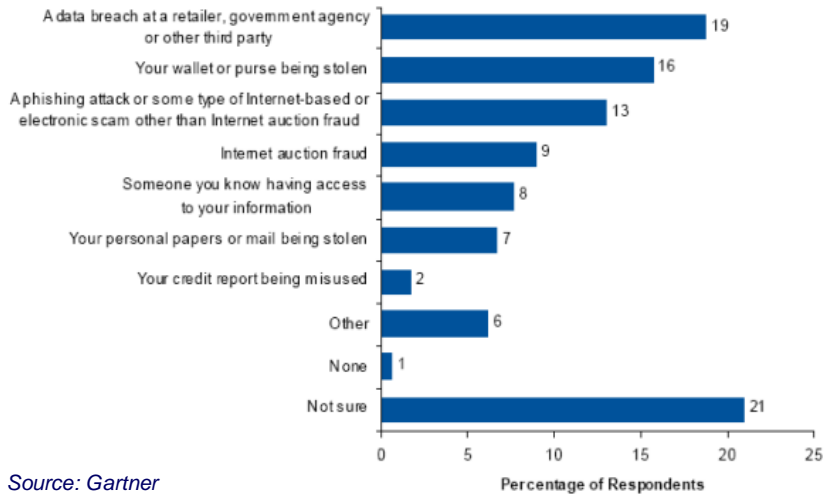
Identify Theft: Victims

- There were 10 million victims of identity theft in 2008 in the United States
- 1 in every 10 U.S. consumers has already been victimized by identity theft
- 1.6 million households experienced fraud not related to credit cards (i.e. their bank accounts or debit cards were compromised)
- Those households with incomes higher than \$70,000 were twice as likely to experience identity theft than those with salaries under \$50,000
- 7% of identity theft victims had their information stolen to commit medical identity theft

Sources: Javelin Strategy and Research, 2009
U.S. DOJ, 2005



Identity Theft: Methods



1st Half 2009 Phishing Activity Trends

- Payment Services surpassed Financial Services as the most targeted sector
- Banking trojan/password-stealing crimeware infections detected increased more than 186% between Q4 2008 and Q2 2009
- Total number of infected computers rose more than 66% between Q4 2008 and Q2 2009, representing more than 54% of scanned computers
- The number of hijacked brands (corporate identities) ascended to a high of 310
- In Q1 2009, more new strains of rogue anti-malware were created than in all of 2008

Source: APWG Phishing Activity Trends Report 1st Half 2009



What might we see in 2010?

- Increase in threats related to:
 - ✓ Social Networking Sites
 - ✓ Banking Security
 - ✓ Botnets
 - ✓ Attacks on users & businesses along with applications
 - Malware attacks - Microsoft & Adobe applications in particular
 - Email attacks will continue to grow via attachments or links
- Increase in the effectiveness of law enforcement to fight back against cybercrime

Source: McAfee 2010 Threat Predictions



Symptoms of Spyware and Viruses

- Computer instability; operating system slows down and hangs up
- Dramatically slower network speed
- Barrage of pop-ups
- New tool bars appearing in your Web browser
- A new homepage appearing when you open your browser
- New and unexpected icons on the system tray at the bottom of your computer screen
- Keys that don't work (for example the "tab" key might not work when you use a web form)
- Random error messages
- Sluggish or downright slow performance when opening programs or saving files



Identify Theft: Recovery

- It can take up to 5,840 hours (the equivalent of a full-time job for 2-years) to correct the damage from ID theft, depending on the severity of the case
- The average victim spends 330 hours repairing the damage
- Over 50% of victims spend 4-7months to straighten out problems caused by identity theft
- 25.9 million Americans carry identity theft insurance
- After suffering identity theft, 46% of victims installed antivirus, anti-spyware, or a firewall on their computer
- Victims of ID theft must contact multiple agencies to resolve the fraud:
 - ✓ 66% contact financial institutions
 - ✓ 40% contact credit bureaus
 - ✓ 35% seek help from law enforcement
 - ✓ 22% deal with debt collectors
 - ✓ 20% work with identity theft assistant services

Sources: *ITRC Aftermath Study, 2004*
Javelin Strategy and Research, 2009



So What Can We Do?

***PAUSE AND
THINK BEFORE
YOU CLICK!!!***



So What Can We Do?

- Take appropriate fraud precautions
- Educate yourself on key evolving schemes
- Become an advocate in educating others

“ . . . realize that the human being is the most important part of any security system equation” Ed Dickson, fraudwar.blogspot.com



Best Practices: Appropriate Fraud Precautions

- Keep your computer current with the latest patches and updates
- Make sure your computer is configured securely
- Choose strong passwords, keep them safe and change them routinely
- Protect your computer with security software
- Protect your personal information
 - ✓ Phony email messages
 - ✓ Fraudulent Web sites
 - ✓ Privacy policies
 - ✓ Guard your email address
- Online offers that look too good to be true usually are
- Review bank, credit card statements and credit reports regularly



Best Practices: Appropriate Fraud Precautions

- Never leave a laptop computer unlocked when not in use
- Think twice about the information you put on a thumb drive
- Don't click "OK", "Agree" or "I accept" to get ride of pop up windows
- Never send personal or confidential information via email and give strong consideration to what you put on social networking sites
- Be suspicious of urgent calls to action that request personal information
- Enroll with a fraud protection service
- Verify the identity of anyone asking for personal information
- Don't click on links or attachments in an email from someone you don't know
- Consider having a separate account to use for "at risk" communication/transactions



What to do if you've been compromised

- Place a "Fraud Alert" on your credit reports and review the reports carefully
 - TransUnion: www.transunion.com 1.800.680.7289
 - Experian: www.experian.com 1.888.EXPERIAN
 - Equifax: www.equifax.com 1.800.525.6285
- Call the security or fraud departments of each company where an account was held and follow up in writing
- Use the Theft ID affidavit to support your written statement
- Ask for verification that the disputed account has been closed
- Keep copies of documents and records of your conversations about the theft
- File a police report
- File a complaint with the FTC
- Reference www.ftc.gov/idtheft for more detailed information



Heightened Awareness

- Routinely review key information sites:
 - www.mcafee.com
 - www.symantic.com/norton
 - www.idtheftcenter.org
 - www.apwg.org
 - www.onguardonline.gov
 - www.ftc.gov/idtheft
 - www.abagnale.com
 - www.annualcreditreport.com
- Discuss and share with:
 - Family
 - Co-workers
 - Friends



“Perhaps we need to take a step back and realize that the human being is the most important part of any security equation. Human beings are on both sides of the equation, whether they are the victim or the victimizer. As long as we continue to maintain information in easily accessible places and send it all over the place, we are going to have a problem.”

--Ed Dickson, fraudwar.blogspot.com



*Lynne Pearson
Vice President
Healthcare Treasury Management
Fifth Third Bank
847.354.7392
lynne.pearson@53.com*