

Senior Seminar

Personal Finance



Classroom Session 5

Lesson V:

Protecting Yourself from Financial Loss

How Can You Manage Risk?

- Risk Avoidance
- Risk Reduction
- Risk Retention
- Risk Transfer

Types of Insurance Policies

- Health / Dental & Vision
- Auto
- Homeowners/Renters (includes Liability)
- Personal Articles (often as a rider on Homeowners/Renters)
- Life
- Disability
- Flood and Earthquake (not covered by Homeowners)
- Umbrella (general Liability coverage)
- Business: Liability / Errors & Omissions / Malpractice
- Secondary (i.e. AFLAC)

Identity Theft

A crime that occurs when someone uses your name, Social Security number, credit card number, or other personal information without your permission.

Methods of Prevention:

- ✓ Guard your personal information – Social Security number, birth date, specific personal information
- ✓ Shred important documents
- ✓ Be cautious when using ATMs and debit/credit card readers
- ✓ Review all monthly financial statements
- ✓ Review your Credit Reports annually

www.annualcreditreport.com

- ✓ Place Fraud Alerts or Security Freezes on Credit Reports
- ✓ Set up online access to your Social Security account

www.ssa.gov/myaccount

- ✓ Use unique Passwords and protect them
- ✓ Use dual-factor authentication, especially on financial accounts

Fraud

Intentional deception to influence someone to part with something of value.

Common Types of Fraud:

- Cashier's check fraud – Craig's List, Marketplaces, etc
- IRS impersonation – The IRS does not call or email, only by US Postal Service
- Social Security Benefits impersonation – Attempts to get your Social Security number and personal information
- Various Phone frauds - Reportedly from a financial institution, police department, computer tech support or anti-virus company

Phishing

An email or pop-up message that seems legitimate and frequently endorsed by a financial institution. The reader is prompted to provide personal information to authorize fixing a problem with an account, product registration, or making a purchase.

Recent Phishing expeditions:

- Impersonating a financial institution webpage (often indistinguishable from the real one) looking for you to input your log-in credentials or account information / PIN
- Impersonating a consumer website, such as Amazon.com, looking to get your log-in information
- Fake website tricking you to click a link that will load a virus or malware onto your computer