Risk Management: Information/Computer Security and Privacy

www.RobertSiciliano.com© 2015

See online handout for complete PPT presentation.

Agenda:

- Hacking for Money
- Perpetrators
- Statistics
- How Stolen Identities Are Used
- The Problem; Identity Theft Types
- How to Obtain an ID
- Legal Forms of ID in Circulation
- Fake Ids
- Public Records
- Privacy Issues
- How a Thief Obtains The Parts
- Prevention Dos' and Don'ts
- Emerging Technologies
- ATM Skimming

Awareness:

- A lack of security appreciation contributes directly to poor security awareness, most notably at the personnel level.
  - This is one of the leading contributors to the human error factor with most security breaches.
  - Security needs to be everyone's business.
  - Corporations and government agencies are directly responsible for protecting personal information entrusted to them by their consumers, so measures must be taken to increase awareness in the everyday IT environment.
  - The most critical step to changing user behavior is to build a secure-minded culture from the ground up.
  - To create this culture, all employees need to be educated and tested on security threats and how their day-to-day computer use behavior can affect their organization's security posture.

Identity Theft Types:

- **New Account Fraud**

Using another's personal identifying information (SSN) to obtain products and services using that person's good credit
standing

- **Account Takeover Fraud**

Using another persons account numbers such as a credit card number to obtain products and services using that
person's existing accounts or extracting funds from a persons bank account.

- **Tax Identity Theft**

Tax-related scams have increased by over 700% since 2008. Two million fraudulent tax returns were filed in 2011 alone,
at a cost of two billion dollars.

- **Child Identity Theft**

Studies show child identity theft is affecting over 500,000 kids every year.

- **Medical Identity Theft**

The deadliest form of identity theft. 1.5 Million victims every year. The motivation of the thief is medical procedures or
any form of attention regarding healthcare

- **Criminal Identity Theft**

Someone commits a crime and uses the assumed name another person. The thief in the act of the crime or upon
arrest poses as the identity theft victim.

- **Business or commercial identity theft**

Using a businesses name to obtain credit or even billing those businesses clients for products and services.

- **Identity Cloning**

Encompasses all forms of identity theft. The thief is actually living and functioning as the victim on purpose

Prevention Don'ts

- Don't leave your wallet/purse in your car
- Don't carry SS cards, birth certificates or passport unless necessary.
- Don't give out your SSN unless you have too
- Don't have SS# or driver's license# printed on checks
- Don't keep PIN #s and passwords in wallet /purse
- Don't use common passwords; mothers maiden, birth date, last 4 of SS or phone, dogs, kids name, consec #s
- Don't put passwords on yellow sticky notes next to your monitor
- Don't write account numbers on the outside of envelopes
- Don't communicate personal information over the phone; SS#, birth date, mothers maiden, CC#

Password Management

- **Dictionary attacks**: These rely on software that automatically plugs common words into password fields. Password cracking becomes almost effortless with a tool like John the Ripper or similar programs.
- **Cracking security questions**: When you click the "forgot password" link within a webmail service or other site, you're asked to answer a question or series of questions. The answers can often be found on your social media profile. This is how Sarah Palin's Yahoo account was hacked.
- **Simple passwords**: When 32 million passwords were exposed in a breach last year, almost 1% of victims were using "123456." The next most popular password was "12345." Other common choices are "111111," "1234567," "12345678," "123456789," "princess," "qwerty," and "abc123." Many people use

first names as passwords, usually the names of spouses, kids, other relatives, or pets, all of which can be deduced with a little research.

- **Reuse of passwords across multiple sites**: Reusing passwords for email, banking, and social media accounts can lead to identity theft. Two recent breaches revealed a password reuse rate of 31% among victims.
- **Social engineering**: Social engineering is an elaborate type of lying. An alternative to traditional hacking, it is the act of manipulating others into performing certain actions or divulging confidential information.
- There are a number of ways to create more secure passwords. One option is to create passwords based on a formula, using a familiar name or word, plus a familiar number, plus the first four words of the website where that password will be used. Mix in a combination of upper and lowercase letters, and you have a secure password. Using this formula, your Bank of America password could be "Dog7Bank," for example. (Add one capital letter and an asterisk to your password, and it can add a couple of centuries to the time it would take for a password cracking program to come up with it.)