

# **What's Your Cyber Identity?**

Law Day, PSU, May 05, 2010

Andrew Lavin  
Deputy District Attorney  
Multnomah County DA's Office  
(503) 988-3621

Fred Wiechmann  
Police Officer  
Portland Police Bureau  
(503) 823-4867

*It has never been easier to gather information about someone than it is today. Should you make it even easier for someone to gather information about you?*

## **I. Identity Theft and Your Cyber Identity**

- Identity theft for financial fraud—How does it work?
  - ID thieves build profiles with different pieces of information about a person. It's like putting together a puzzle.
  - The puzzle pieces: full **names**, **maiden** names, **addresses**, **city/state** you live in, **birth** dates, years of **graduation**, **license** numbers, **social security** numbers, **credit card** numbers, **VINs**, **e mail** addresses, **passwords**, info that could supply **answers** to **security questions**, **businesses** you deal with, etc.
  - Profiles are compiled in many forms. Low tech or high tech.
  - Profiles are valuable to thieves—traded like baseball cards.
  - They're traded for drugs (meth), stolen property, or new profiles.
  - The profiles are used to steal from existing accounts or to set up new and fraudulent accounts. They're used to create fake IDs.
- Identity theft for financial fraud—What are the effects?
  - Financial loss or incurring financial liability that isn't yours.
  - Inconvenience for years.
  - Civil or criminal legal liability that shouldn't be yours.
- Identity theft—How can an ID thief use my social network site?
  - They can get a lot of information directly from your page. Think about what's on there: name, age, geographic location, e mail address, interests, biographical information, school, work, etc.
  - They'll request information from you or access the private portions of your page by tricking you—phishing your account by getting you to enter your password or with fake friends requests.
  - It doesn't take much information about someone to access an account or start a new one. They *will* take the time to do it.
  - Access to accounts is often through passwords, e mail and security questions. Think about what happens when you forget your password.
- Identity theft—What else can happen besides financial loss?
  - People could use your account to embarrass you or cause damage to your reputation. This could be done by pretending to be you.
  - It's easy to locate, download and use your pictures against you.
  - Example: the Craigslist/Myspace prostitution case.

**(Continued on other side)**

## **II. Your Cyber Identity and Other Kinds of Crimes**

- Stalking and Violations of Restraining Orders
  - Stalking (Cyber Stalking) is the sending of unwanted emails / text messages to a person
  - Sending emails or text messages to a person who has a restraining order against you is a violation.
- Sex Crimes
  - Child Pornography – Manufacturing, Possessing and Distributing
- Burglary, Robbery and Assault—knowing too much about your locations and activities.
  - Listing where you go to school / Work / live.
  - Listing what you are doing at that time (i.e. Facebook comments.)

## **III. What You Can Do to Protect Yourself**

- Set your profiles to private. However, even then you should be mindful of what you post.
- Do not display your full name, birth dates, e mail addresses, or any numbers associated with you. Limit info on biography and interests that could lead to your passwords or answers to security questions.
- Don't friend people you don't know and trust. Verify all friend requests you get from someone you think you know. Is it really them?
- Don't provide information to others who ask you for it over the internet.
- Be conservative about the pictures you place on your page.
- Be careful where and when you enter your password—phishing!
- Vary your passwords from site to site and change them often.
- Be responsive if you're victimized: call the police if you think it is a crime, notify the service provider, inform credit reporting agencies if it's fraud.

## **IV. Other Ways Your Information Can be Accessed and Used**

- Family, employers, prospective employers, school admissions, school administrators and law enforcement may be watching.
- The next step—requirements to disclose. Federal employers do it.
- Law enforcement uses the information as evidence, regularly. Service providers keep the information and respond to subpoenas.
- Attorneys are using it against people who are witnesses

## **V. Things to Keep in Mind**

- Always be cautious and vigilant. Protect yourself at all times.
- What do you want people to know and who do you want to know it?
- The more you post, the more you risk.
- You're creating a record of your activities—a "paper trail".
- The laws and security measures haven't caught up with the risks.
- Whatever you do on a computer is always recoverable. This is the same for cell phones they are nothing more than little computers.