# Self Directed Training within a Cyber World

Paul Krasley
March 26, 2009

This briefing is classified
UNCLASSIFIED

# Introduction

- This presentation is not about
  - Validating on the server
  - Using absolute path and filenames
  - Avoiding real directory and files
  - HTML tags
  - Stripping special and invisible characters
- It is about, changing your mind set and
  - There are people who want your information, and will do anything necessary to get it
  - Nothing you do in the unclassified world – online or mobile is safe or private
  - You must protect your information like your protect your wallet
  - Technology is not going away, so how to use technology as safely as possible is the key

# The Risk

- How many of you have or your family have?
  - Cell phone (handheld and car), PDA, two-way pagers, & MP3
  - GPS
  - Home PC shared by family members
  - More than 3 credit cards
  - Been the victim of identity theft or know someone who has
  - Family, friends, and associations (professional/private)

- How many of you
  - Use Facebook, Interlink, or social networking sites
  - Play online games
  - Attend trade shows, school, publish, or make presentations

**There is no guarantee of privacy in “any” wireless system!**

# Threats

- FIS, Crime, and Terrorism
  - Significant foreign embassy presence and FIS activity
    - **They seek advantages in military, economic, political, technology, and education**
    - **They will use anything they can against you**
  - Computers
    - **Use of the internet & cyber crime (biggest cyber concern)**
    - **Covert communications, fund raising, banking, planning, mgt., recruiting**
  - Sensitive albeit unclassified intrusions 37,000 (DHS, 08)
  - Cyber attacks = $226 billion (CRS)
  - Lost revenue = $40 billion
  - Lost $8 billion as a result of viruses, spyware, and phishing

# Threats

Counterintelligence and Security

Myspace.com

Blogger

Flickr

Linkedin

Craiglist

Pay Pal

Ebay

Classmates.com

You Tube

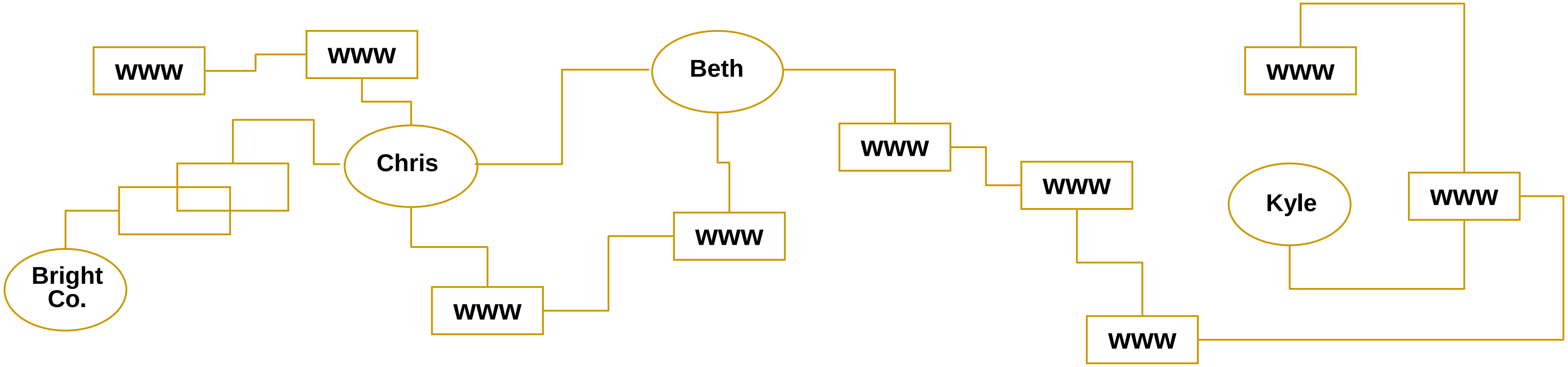
Blogspot.com

Twitter

Facebook

2nd Life

World of Warcraft



# Spear Phishing

- Spear Phishing
  - One of the top ten most common virtual attacks
  - Can happen at the office (Intel) and at home (identity theft)
  - Can include malicious software

A Red Team sends an email "This e-mail contains a virus and an attachment called "Do Not Open"

**68%** open the email

**23%** open the attachment

**The goal is to get you to open the attachment or click on a link**

# Critical Information

- What they want
  - Full Name
  - SSN
  - Date and place of birth
  - Home address
  - Home phone number
  - Email accounts and IP addresses
  - Financial account numbers and institutions
  - Driver’s license number and state
  - Vehicle registration information

# Critical Information

- Work Related
  - Agency or company name
  - Specific office or division name, information, and location
  - Your specific job duties, titles, grade, or rank
  - Office phone number
  - Email addresses
  - Previous duty assignments
  - Photos of work locations
  - Information related to work operations, jobs, assignments, and co-workers
  - Information regarding travel for work (past or future)
  - Specific capabilities, limitations and vulnerabilities
  - Specific communications, and security procedures
  - Operating locations
  - Specific equipment or unique location

# What you must Do!

Counterintelligence and Security

- Social Networking
  - **Google** yourself
  - Six degrees of separation
  - Never use a cyber café or open access
  - You leave a trail and does your family
  - Talking around a topic often points to it
  - Sometimes the connection is by what you don't say
  - Do you really know who you are talking to

**Once you Say It, Push Enter or Click Send it is gone FOREVER!**

# What you must Do!

- Disable automated preview
- Read email messages in plain text
- Do not click on embedded links
- Enter the web address directly
- Do not open emails from unknown sources
- Use PKI and tell others to
- Ask yourself why am I sharing this information
- What will they do with the information
- How are they protecting the information

**“The reason evil triumphs, is because good men do nothing” (Edmund Burke).**

# What you must Do!

- When traveling, at a conference, or anywhere else
  - Keep your laptop, phone, PDA, & other devices with you at all times
  - Never “trust” anyone, your hotel or their safe
  - Beware of customs and other checkpoints
  - Remove the hard drive, or SIM card or disable the device
  - Use encryption, strong passwords, and change them often
  - Do not have unnecessary information stored

Using public sources openly and without resorting to illegal means, it is possible to gather **“at least 80%** of the information about the enemy” – Al-Qaeda terrorist training manual

# Protecting Yourself

- ISP
  - Get to know your ISP and their Security
- PC
  - Firewall
  - Operating system up to date
  - Anti-virus and spyware installed
  - Spam Filter
- Browser Maintenance
  - Delete Cookies, Files, and offline content
  - Security setting to high and use trusted sites
  - Privacy tab – default
  - Block pop-ups
  - Control Active X

# Protecting Yourself

- Passwords
- Screen Lock
- Password at Start Up
- Be a user and not admin
- Encryption
- Close windows with the X
- Work only in https
- PKI
- Do you really know who you are talking to
- Why are you telling them this information
- What will they do with it

# Take Aways

- Nothing you do in the unclassified world – online or mobile is safe or private
- Google yourself
- Six degrees of separation
- Why do they need to know
- Why am I sharing this information
- What will they do with the information once shared

Paul Krasley
paul.krasley@dia.mil
(703) 907-2726

# Spear Phishing

- Look for
  - Generic Greeting
  - Fake Sender’s Address
  - False Sense of Urgency
  - Fake or deceptive web links
    - **Email is requiring that you follow a link to sign up for a great deal, or to log in and verify your account status, or encourages you to view/read an attachment**
  - Email that appear like a website
  - Misspellings and bad grammar