It’s Go Time *Robots Attack* Family Internet Safety

Paul Krasley
March 25, 2009

This briefing is classified

UNCLASSIFIED
“At a Glance”
Graphic Narrative
Visual Storytelling

Translates to multi-media
Appeals to all ages
Works in any context
Conveys depth & complexity
Simplicity = emotional impact
Audiences wanting more
Enhance Branding
Introduction

- There Is No Privacy
  - Protect your information as you protect your wallet or purse

- 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
  - Has family, friends, and associations
  - Use Facebook, Interlink, or social networking sites
  - Play online games
Threats

Myspace.com
Blogspot/Blogger (DOB)
Flickr (Pictures)
Linkedin (Groups)
Craigslist (Selling)
Pay Pal (Online Payment)
Ebay (Buy/Sell)
Geolocation (IP Tracking)
CriminalSearches.Net (Speed Tkts)

Classmates.com
You Tube
Slashdot (Location)
Twitter (Twits = GPS Loc.)
Facebook (13 Billion Pictures)
2nd Life
World of Warcraft
Vehix (Selling a Car)
Lessons from “Comic Book”

- BotNet = PC Slow = Firewall
- Camera = On/Off = Seen/Unseen
- Malware = Secret SW = Missing Data
- Viruses = Problems = Auto Scan
- Internet Cache = Cookies & History = No Trail
- Email = Friends = How Do You Know
  = Links = Trouble
- Online = Records Somewhere = Your Future
- Online Profile = What Does It Say About You
- Internet Contract = Good OPSEC = Family Security
What users say about “Comic Book”

- 6 to 14 year olds and up
  - Best comprehended by 9 to 14 year olds
  - “Even though I thought I knew everything about internet safety, I learned a lot from this still” (DIA, Dependent)
  - “My Dad told me webcams were unsafe”
  - “Peer pressure is a really good topic to cover! It’s a very important issue and SO true!”
  - “Have all the members sign a contract”
  - “Someone you can trust…Mom, Dad, Gramma, not best friend Jimmy”
  - “Three magic questions…great reference, on the computer, texting, or whatever and easy to remember!”
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

- Got a Mailbox with a RED Flag?

Can you think of others?
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

Can you think of others?
What You Must Do

- Think like a Thief
- Reduce your electronic footprint
- Google yourself
- Six degrees of separation
- Never use a cyber café or open access
- You leave a trail and so does your family
- 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
- Become “click shy”
- Find out what your friends and family know about security
- Have an Internet Security Party

The goal is to get you to open the attachment or click on a link
What You Must Do.

- When traveling
  - 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

- Passwords
- Screen Lock
- Password at Start Up
- Be a user and not admin
- Encryption
- Close windows with the X
- Work only in https
- Disable or limit folder & printer “sharing” options
- Save sensitive files in an encrypted archive file
- When surfing…close MS Office Programs

You need to “play” offense
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
  - Disable Unneeded Software

- **Browser Configuration & Maintenance (Firefox)**
  - Delete Cookies, Files, and offline content
  - Settings: bullet next to “Every Visit to Page”
  - Security setting to high and use trusted sites
  - Privacy tab – default
  - Block pop-ups
  - Control Active
Persona
Who you are on the internet

Computer
- IP Address
- Operating system version
- Operating system language
- Clock time

Clipboard
- Your clipboard can be viewed by the site you visit
  What you copy and paste?
  - passwords
  - web addresses
  - physical addresses
  - names
  - sensitive search terms

HTTP Referer
- Identifies URL of the previous webpage from which a link was followed

Browser
- Version
  - Who was last to use Netscape?
  - What does DoD use?
- Title
- History: sites visited within a “session”.
  Session can last life of account to yrs.

Cookies
If you fill out a from this info MIGHT be in a cookie:
- Your name
- Address
- Email
- Credit card number
- User preferences
- Web surfing behavior
- Contents of electronic shopping carts
- Website you have visited
**Persona**

**Who you are on the internet**

**Browser information – [http://browserspy.dk](http://browserspy.dk)**

<table>
<thead>
<tr>
<th>Accepted Filetypes</th>
<th>Email Verification</th>
<th>Objects</th>
<th>Silverlight</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveX</td>
<td>Flash</td>
<td>Object Browser</td>
<td>Sound Card</td>
</tr>
<tr>
<td>Adobe Reader</td>
<td>Fonts via Flash</td>
<td>Online/Offline</td>
<td>SVG</td>
</tr>
<tr>
<td>Ajax Support</td>
<td>Fonts via Java</td>
<td>OpenDNS</td>
<td>Text Formatting</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Gears</td>
<td>OpenOffice.org</td>
<td>File Upload</td>
</tr>
<tr>
<td>Browser</td>
<td>Gecko</td>
<td>Opera Browser</td>
<td>UserAgent</td>
</tr>
<tr>
<td>Capabilities</td>
<td>Geolocation</td>
<td>Operating System</td>
<td>VGScript</td>
</tr>
<tr>
<td>Colors</td>
<td>Google Chrome</td>
<td>Google PageRank</td>
<td>WAP Device</td>
</tr>
<tr>
<td>Components</td>
<td>GZip Support</td>
<td>HTTP Password</td>
<td>WebKit</td>
</tr>
<tr>
<td>Connections</td>
<td>HTTP Headers</td>
<td>Ping</td>
<td>Window</td>
</tr>
<tr>
<td>Cookies</td>
<td>HTTP</td>
<td>Plugins</td>
<td>Windows Media Player</td>
</tr>
<tr>
<td>CPU</td>
<td>Images</td>
<td>Plugs</td>
<td></td>
</tr>
<tr>
<td>CSS</td>
<td>IP Address</td>
<td>Plugins</td>
<td></td>
</tr>
<tr>
<td>CSS Exploit</td>
<td>Java</td>
<td>Prefetch</td>
<td></td>
</tr>
<tr>
<td>Cursors</td>
<td>JavaScript</td>
<td>Proxy</td>
<td></td>
</tr>
<tr>
<td>Date and Time</td>
<td>Languages</td>
<td>Personal Security Manager</td>
<td></td>
</tr>
<tr>
<td>DirectX</td>
<td>Mathematical</td>
<td>QuickTime Player</td>
<td></td>
</tr>
<tr>
<td>Document</td>
<td>MathML Support</td>
<td>RealPlayer</td>
<td></td>
</tr>
<tr>
<td>.NET Framework</td>
<td>MIME Types</td>
<td>Resolution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mobile</td>
<td>Screen</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shockwave</td>
<td></td>
</tr>
</tbody>
</table>
Persona

Who you are on the internet

Browser information

ActiveX: ....................... is activeX available and active on your browser
Browser: ....................... name, version, layout, operating system
Cookies: ....................... are cookies enabled and supported in the browser, type of cookies
CPU: ......................... what central processing unit (cpu) your system has
CSS Exploit: ............... detect which sites you have been visiting lately
Date and Time: .......... time and date on your system
Email Verification:....... find out if your email address can be verified; mail server setup
Fonts: ....................... find out which fonts your system has installed using Flash and Java
Geolocation: ............... find out where in the world you are; based on IP address
Images: ...................... which image formats your browser supports
IP Address: ............... what your IP address is
Languages: ................. which languages your browser supports and which languages it says it accepts
Operating System: ...... which operating system you are using
Plugings: .................... which plugins your browser has installed
Proxy: ....................... if you are using a proxy to connect to the internet
Resolution and Screen Size: ............... information about your screen
Security Information: ..... encryption strength
Take Away

- 3 Magic Questions
  - Why are you sharing the information?
  - What is the person going to do with the information?
  - How will the information be stored

- Family Internet Contract

- Back Up, Back Up, Back Up

- You Don’t Leave Your Front Door Open. Do You?

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