Managing Your Top Human Risks

Lance Spitzner
securingthehuman.sans.org
lspitzner@sans.org
@securethehuman
Security Awareness Maturity Model

- Compliance Focused
- Promoting Awareness & Behavior Change
- Long-Term Sustainment & Culture Change
- Metrics Framework

Non-existent
BJ Fogg Behavior Model

Fogg Behavior Model

B = mat

behavior motivation ability trigger
at same moment

High
Motivation

motivation

Low
Motivation

Hard to Do

ability

Easy to Do

triggers

succeed here

Action Line

triggers

fail here

www.BehaviorModel.org

© 2007 BJ Fogg

For permissions, contact BJ Fogg
Start with WHY

• Why does cyber security matter?
• Communicate at an emotional level, do not rationalize
• Focus on personal benefit
Keep it Short

Focus only on the topics that have the greatest ROI

- People can only remember so much (cognitive overload)
- You have limited time & resources
- Fewer topics easier to reinforce
- Avoid ‘training fatigue’
- Costs
<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Crimeware</th>
<th>Cyber-espionage</th>
<th>Denial of Service</th>
<th>Everything Else</th>
<th>Stolen Assets</th>
<th>Misc. Errors</th>
<th>Card Skimmers</th>
<th>Point of Sale</th>
<th>Privilege Misuse</th>
<th>Web Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation (72), n=282</td>
<td>1%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>95%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Educational (61), n=29</td>
<td>7%</td>
<td>17%</td>
<td>17%</td>
<td>27%</td>
<td>3%</td>
<td>50%</td>
<td>3%</td>
<td>30%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Entertainment (71), n=38</td>
<td>1%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>47%</td>
<td>4%</td>
<td>82%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Finance (52), n=795</td>
<td>3%</td>
<td>3%</td>
<td>11%</td>
<td>19%</td>
<td>22%</td>
<td>7%</td>
<td>32%</td>
<td>3%</td>
<td>1%</td>
<td>57%</td>
</tr>
<tr>
<td>Healthcare (62), n=115</td>
<td>1%</td>
<td>3%</td>
<td>4%</td>
<td>25%</td>
<td>1%</td>
<td>3%</td>
<td>11%</td>
<td>24%</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Information (51), n=194</td>
<td>4%</td>
<td>47%</td>
<td>3%</td>
<td>1%</td>
<td>3%</td>
<td>24%</td>
<td>1%</td>
<td>21%</td>
<td>57%</td>
<td></td>
</tr>
<tr>
<td>Manufacturing (31-33), n=37</td>
<td>3%</td>
<td>25%</td>
<td>4%</td>
<td>21%</td>
<td>4%</td>
<td>13%</td>
<td>1%</td>
<td>13%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Professional (54), n=53</td>
<td>12%</td>
<td>16%</td>
<td>4%</td>
<td>9%</td>
<td>37%</td>
<td>13%</td>
<td>13%</td>
<td>9%</td>
<td>2%</td>
<td>26%</td>
</tr>
<tr>
<td>Public (92), n=193</td>
<td>1%</td>
<td>1%</td>
<td>4%</td>
<td>1%</td>
<td>3%</td>
<td>64%</td>
<td>2%</td>
<td>2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail (44-45), n=182</td>
<td>1%</td>
<td>1%</td>
<td>4%</td>
<td>1%</td>
<td>3%</td>
<td>64%</td>
<td>2%</td>
<td>2%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Top Topics / Risks

- Phishing
- Passwords
- Accidental
Phishing
Dear Customer,

Unfortunately we unable to deliver your package this morning. We will be making two more attempts in the next 48 hours. If we are unable to deliver your package we will then have to return to sender. Please verify that your delivery address is correct by clicking on the link below, or updating the attached document.

Order# 44187
*****************************************************************************
Shipping Tracking Information
*****************************************************************************
Shipping Provider: UPS
Tracking #: 1Z9Y424V039787851X
Tracking Information: http://www.ups.com/tracking/1Z9Y424V039787851X
Ship Date: 18/10/2012

Thank you,
United Parcel Service

PackageTracking.pdf (91 KB)
Behaviors

- Identify the indicators of a phishing attack.
- Explain the actions to take
- Explain how to report an attack
- Do they feel comfortable reporting? Do they feel action will be taken?
Passwords
Typical Password Training

- Minimum 12 characters
- 1 symbol
- 1 number
- 1 capital letter

Change every 90 days
  - Costs associated with this
What are We Missing?

• Do not get infected
• Do not share your passwords
• Do not login using untrusted systems
• Personal questions for password reset
• Passphrases – *Where is my Coffee?*
• Different passwords for different accounts (encourage password managers)
• Use dual factor authentication when possible
Accidental
Accidents

Far too often forget about accidental.

- Auto-complete in email
- Forgetting documents in the taxi or your laptop at airport security
- Loosing your mobile device
Upcoming Events

• Monthly Webcasts
• Security Awareness Summits
  – London: 11 Nov
• SANS MGT433 Courses

securingthehuman.sans.org/events