Gamification and Other Creative Measures for Improving Security Awareness

Ira Winkler
ira@securementem.com
+1-443-603-0200
Captain Kirk

• Who wouldn’t guess a password of “Captain” on an account with the user ID, “Kirk”?
• This happened at NSA
Who’s Fault Is It?

• She sounds like an idiot
• She is an Ivy League graduate
• Why was she not previously told that she shouldn’t have that as a password?
• Why was the password allowed in the first place?
This Is Not Unique

• Security professionals make assumptions in the base level of knowledge in end users
• Also extends to knowledge assumptions about other technical professionals
• As per Felix Unger, when you assume you make an ass/u/me
Common Sense

• The problem is that security professionals assume that the users should exercise common sense
• There is no such thing as common sense without a base common knowledge
• Security programs fail, because they assume there is the common knowledge
It’s Not Stupid Users

• It’s incompetent security professionals
• While there are some stupid activities on the part of the users, I always ask what could the security staff have done better?
• Does your staff stop and ask how could the incident have been prevented
• Is there a discussion of both modifying user activity and preventing user activity
The Culture Chain

• Awareness creates behaviors
• Behaviors create culture
• Culture creates or reduces security incidents
• Culture allows for slower or faster mitigation
• Culture costs or saves the organization money
Motivation: The Critical Failing

• You need to ensure that users have motivation to ensure they take action
• Motivation is what changes logical knowledge to physical action
• Experiences create motivation when done properly
• Motivation solidifies culture
Verifying Awareness Training Compliance
Traditional Security Awareness Programs

• Typically pushes information to users
  – Videos, posters, newsletters, etc.
  – Little tracking of usage

• Forces users to take training
  – Only metrics are Pass/Fail

• Focuses on topics
• Great for some environments
What Really is Security Awareness?

• Confusion of Training vs Awareness
• Training provides a fixed body of knowledge and possibly tests for comprehension
• Awareness is about changing behavior
• The only way to measure awareness is by measuring real behaviors
Why Does Awareness Fail?

• Most awareness programs aren’t
  – Training, not awareness
  – Single training tools used

• Provide information and measure short term comprehension

• Information does not mean action

• All security measures will fail, but need to be put in perspective
THE HABITS
Habit 1 – Create a Strong Foundation

• This is the main source of failure
• Make a 3-month plan
• Topics may change
• Assess Approach
  – Softball
  – Hard push
  – Avoid fear-mongering
Choosing Components

• Which mediums of communication will be most effective at your company?
• Which mediums are already saturated?
• What are employees most receptive to?
Potential Components

- Website
- Posters
- Newsletters/Blog
- Monthly tips
- Lunch and Learns
- Roadshows
- Speakers
- Security Week
Keep The Program Fresh

• Easy to fall behind
• Pay attention to the news
• Create new material for every month
Habit 2 – Organizational Buy-In

• Appeal to the highest level you are able to engage
• Market some materials to the C-level
• Stress benefits of Security Awareness
Habit 3 – Participative Learning

• Learning modules
• Interactive components/Gamification
  – Make user feel involved
• Additional tools
  – Phishing
  – Other “Teachable Moments”
Habit 4 – More Creative Endeavors

• Guerilla marketing campaign
• Security Cube
• Policy distribution
• Demonstrations and movie showings
Habit 5 – Gather Metrics

• No participating company gathered metrics
• Compare rate of reported incidents pre and post
  – Collecting metrics ahead of time so you can potentially measure success after the fact
Assessing Success

• Assess which components have been successful
• Administer a survey
  – Try to keep it anonymous
  – Offer a drawing that employees can enter for a prize
• Understand limitations
Habit 6 – Partner With Key Departments

• Reinforces company message vs. security message
• Consider departments such as:
  – Legal
  – Compliance
  – Human Resources
  – Marketing
  – Privacy
  – Physical Security
Habit 7 –
Be The Department of How

• Department of “How” vs. Department of “No”
• Teach instead of dictate
• Establish positive security culture
What is Gamification?

• The application of game principles to business problems
• Encouragement of participatory engagement and voluntarily seeking out additional information
• Not limited to business problems
  – Getting wide use in fitness, training and marketing
Common Gamification in the Real World

• Airline frequent flier programs
• LinkedIn participation
• TripAdvisor and Yelp badges
• Hotel frequent traveler programs
  – Gas rewards, discounts only to club members
• Nike+
• Starbucks app
What They All Strive to Do

• Create brand loyalty
• Reward for extra purchases
• Encourages more of the desired behaviors
• Completely voluntary
What is Gamification of Security Awareness?

- A long-term, ongoing awareness program
- Focuses on behaviors
- Proactively rewards good security behaviors
- Encourages employees to seek out awareness training and opportunities
  - Gets employees to ‘pull’ awareness materials
- Reverses the awareness program paradigm
What Is NOT Gamification?

- An actual game
- A one-time effort
- Video based training
- Phishing simulations

*If you force users to take the “gamified” training, it is not gamification!*
Principles of Gamification

1. Clearly defined goals
2. Rules/limitations
3. Ongoing feedback
4. Voluntary participation
Clearly Defined Goals

• Clearly identified goals
• Clearly identified rewards for hitting the goals
• Goals are achievable
• Rewards are desirable
Rules

• Define how participants attain the goals
• Creates limitations for achieving goals
• Limitations make it engaging
• Think carrying the ball in golf or soccer
Feedback

- Participants know how they are doing towards achieving their goal
- Organization knows which employees deserve rewards
- Feedback mechanism can entice further participation
Voluntary Participation

• No one is forced to participate in program
• Rewards encourage participation
• With most gamification programs the challenge is the reward
  – Think golf
How Do You Create a Gamification Program?

- Assess your culture
- Examine your business drivers
- Identify a theme to create the program around
- Set up system to record points
- Create awareness of your program
Culture Determines Reward Structure

- What will incentivize your employees to participate in your program?
- What will upper management allow you to give?
  - Gift cards, acknowledgment, free lunch, gifts, days off
- Tiering the reward structure
  - Easy for basic rewards
  - Attainable for advanced rewards
  - Requires work for ultimate reward
Business Drivers Determines Point Structure

• What behaviors do you reward?
• What activities do you reward?
• How many points for each?
  – For example, if stopping tailgaters is a big priority for your organization, you should award more points for that than reading an article
## Sample Point Structure

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Points Awarded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read article</td>
<td>50</td>
</tr>
<tr>
<td>Forward phishing message</td>
<td>50</td>
</tr>
<tr>
<td>Attend lunch and learn</td>
<td>100</td>
</tr>
<tr>
<td>Stop tailgater</td>
<td>100</td>
</tr>
<tr>
<td>Report social engineering attempt</td>
<td>100</td>
</tr>
<tr>
<td>Find security vulnerability</td>
<td>200</td>
</tr>
<tr>
<td>Give presentation</td>
<td>250</td>
</tr>
</tbody>
</table>
## Sample Reward Structure

<table>
<thead>
<tr>
<th>Level</th>
<th>Points</th>
<th>Reward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginner</td>
<td>100</td>
<td>Badge, T-shirt</td>
</tr>
<tr>
<td>Apprentice</td>
<td>500</td>
<td>Badge, gift card, certificate</td>
</tr>
<tr>
<td>Group Expert</td>
<td>1,000</td>
<td>Badge, executive acknowledgement, bigger gift, advisor status</td>
</tr>
<tr>
<td>Expert</td>
<td>2,000</td>
<td>Badge, C-level acknowledgment, more money, more shwag</td>
</tr>
<tr>
<td>Guru</td>
<td>3,000</td>
<td>Badge, promotion, day off...Make it worth it!</td>
</tr>
</tbody>
</table>
Tracking Infrastructure

• You need a way to keep track of everyone’s points
• Tracking can be more difficult than the rest of the program
Putting It Together

• Takes some effort to figure it all out
• The roll out strategy is not as easy as it may seem
• You need to determine the appropriate effort
• Might be all or just part of your awareness program
More Creative Measures - Games

• Contests
  – Video contests, writing articles, etc

• Experiences

• Virtual experiences

• Teachable moments
  – Phishing, USB drops, Social Engineering
  – Be aware of political sensitivities, gothcha implications, people feeling picked on
Events
Virtual Events
Conclusions

• Gamification is better for some environments than others
  – Tech people with more autonomy tend to respond better to gamification
  – Not everyone needs to participate
• You can have multiple programs
• Culture drives reward structure and rewards
• Business drivers and security concerns drive points
• Reverses the security awareness program paradigm
Conclusions Continued

• Most awareness programs aren’t
• If you want an effective program
  – You must strive to change behaviors
  – You must be holistic
• Tailor the program for organizational culture
• Creativity is awesome, more than pushing materials required
• Focus on reinforcing Common Knowledge so your users can demonstrate Common Sense
For More Information

http://www.securementem.com
    @securementem

http://www.irarireport.com
    @irarireport

ira@securementem.com
    +1-443-603-0200
www.facebook.com/ira.winkler
    @irawinkler
www.linkedin.com/in/irawinkler