Using Gamification to Transform Security Awareness
SANS Security Awareness Summit, London 2016

Masha Sedova
Senior Director of Trust Engagement, Salesforce
@modMasha
About me

• Background in security with a love of behavior psychology, human motivation, and behavioral economics.
• I’ve been building Salesforce’s Trust Engagement team since 2012.
• Run a team responsible for general employee security culture, secure development and engineering practices, and customer security advocacy.
• Passionate about using transforming security behaviors from “have to” to “want to” by looking at the full scope of an employee’s experience.

Life is not a dress rehearsal.

Rose Tremain
What Does Security Awareness Mean To Your Organization?

Often our requirements are very general

I want my employees to:

- Make less security mistakes
- Have more security common sense
- Be more vigilant
- Care more about their actions
What Are Your Key Behaviors?

Ask: What behaviors am I trying to change?

Ask: What will people do differently after my effective program is in place?

Ask: How will I measure this?
How To Prioritize Key Behaviors

1. What are your most frequent incidents?
2. What would be the most damaging to your company?
3. What are easy wins?
4. What’s most visible?
5. What would have the greatest impact on your security posture?
6. What does your team already have metrics on?
Linking Results to Key Behaviors

Think like a Chief Security Officer

- # of Security Champions in Org

See something, say something

- # of people who detect and report a vulnerability

Say no to badge surfing

- # of unauthorized people accessing secure areas

Don’t get fooled by Phishing

- # of people who fall victim to a phishing attack

Get certified and be ready

- # of employees who completed annual security training
Investigate Root Cause
Why are these behaviors not being done?

- Can this be solved with technology?
  Do it! Changing mindset is the hardest way to go about enforcing change.

- “I didn’t realize that security was part of my job.”
  Communication, marketing, awareness campaigns

- “I didn’t know what to do about it.”
  Training and skills

- “I didn’t have the resources or support to do it.”
  Management alignment

- “I didn’t want to.”
  Gamification and incentives
When I Say Security, You Say...
Unleashing Discretionary Performance
It’s Not About Playing Games At Work
Gamification Elements

1. **Autonomy**: we like having choices
2. **Mastery**: we like getting better at what we do
3. **Feedback**: we like getting feedback on how we are doing
4. **Purpose**: meaning amplifies what we do
5. **Social**: all this means more with others
Gamifying Security

- Pick Vital Behaviors
- Connect to Purpose
- Test And Give Feedback
- Reward/Recognize or Educate
- Socialize
Key Behaviors: Phishing, Reporting, and Badge-Surfing

DON'T GET FOOLLED BY

SOMETHING,
SAY SOMETHING.

SAY NO TO BADGE-
Connect to Purpose

CYBER CRIME VICTIMS

556 MILLION PER YEAR

1.5+ MILLION PER DAY

18 PER SECOND_

Source: Verizon Breach Report 2014
Connecting to Purpose

Employees experience how attackers exploit “bugs in human hardware”

“Can you hold that office door open for me, my arm’s broken and this package is heavy.”

“Holy wow…Check out this video of a giant snake eating a zoo keeper!”

“If you don’t pay the fine, your files will be locked and you will be reported to the FBI!”
Test With Feedback
Recognizing Badge-Surfing Awareness

THANK YOU
FOR SAYING NO TO
BADGE-SURFING.

LETS GET YOU
REWARDED!

Post a photo of yourself holding this card on Chatter with @Security and #StrongestLink to receive your Jedi points & prizes.

SECURITY
Be the strongest link.
Recognizing Reporting

Benjamin to Christine

Thanks for reporting an email you found suspicious to the CSIRT. Your demonstrating our #1 value #TRUST

Learn more about reporting suspicious activity at https://sites.google.com/a/salesforce.com/csirt/report

Want to learn more about Trust points and Jedi Badges?
http://intranet.internal.salesforce.com/departments/security/Jedi_Program.html

@Daniel @Masha Sedova @Warwick

Masha Sedova to Christine

Well done on earning the first security champion level! Stay Paranoic!

@Daniel @Benjamin

apprentice
Beware the Dark Side, young Level 1 Security Apprentice

trust_points_100
Congratulations! You've earned 100 Trust points.
# Reward: Security Champion Program

<table>
<thead>
<tr>
<th>Level</th>
<th>Skill</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apprentice</td>
<td>Basic awareness</td>
</tr>
<tr>
<td>Padawan</td>
<td>Successful Testing</td>
</tr>
<tr>
<td>Knight</td>
<td>Doing</td>
</tr>
<tr>
<td>Master</td>
<td>Teaching</td>
</tr>
<tr>
<td>Grand Master</td>
<td>Innovating</td>
</tr>
</tbody>
</table>

## Trust Points

- 100
- 200
- 300
- 400
- 500
- 600
<table>
<thead>
<tr>
<th>Item</th>
<th>Point Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiving a Trust badge</td>
<td>50</td>
</tr>
<tr>
<td>Read security newsletter and chatter about it</td>
<td>50</td>
</tr>
<tr>
<td>Reporting phishing email/ social engineering call</td>
<td>100</td>
</tr>
<tr>
<td>Completing 100 level course</td>
<td>100</td>
</tr>
<tr>
<td>Completing 200 or 300 level course</td>
<td>200</td>
</tr>
<tr>
<td>Identifying a vulnerability (P0 - P3)</td>
<td>P0 =500, P1=300, P2=200, P3=50</td>
</tr>
<tr>
<td>Attending a Security lunch and learn</td>
<td>200</td>
</tr>
<tr>
<td>Winning a bug bounty event</td>
<td>500</td>
</tr>
<tr>
<td>Attending hands-on security training course</td>
<td>600</td>
</tr>
<tr>
<td>Teaching/Presenting on Security topic</td>
<td>1000</td>
</tr>
<tr>
<td>Presenting at Conference on Security</td>
<td>2500</td>
</tr>
<tr>
<td>Security Patent</td>
<td>3000</td>
</tr>
<tr>
<td>Interning with Trust</td>
<td>3000</td>
</tr>
</tbody>
</table>
Creating effective leaderboards

- New participants should see the impact of their progress on leaderboards
  - Same 5 people were on top with little rotation.
- Post leader of the week or per activity.
- Have points that expire.
- Consider the experience for the other 90% of participants who don’t top the chart.
  - Does it become demotivational?
Incentives and Rewards

- Competition
- Achievement
- Status
- Self-Expression
- Altruism
- Access
Creating effective point systems

<table>
<thead>
<tr>
<th>Sample Motivation Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Training</td>
</tr>
<tr>
<td>SEC 101</td>
</tr>
<tr>
<td>SEC 201</td>
</tr>
<tr>
<td>Security Behaviors</td>
</tr>
<tr>
<td>Report Phishing Emails</td>
</tr>
<tr>
<td>Identify a Vulnerability</td>
</tr>
<tr>
<td>Level System</td>
</tr>
<tr>
<td>Jedi</td>
</tr>
<tr>
<td>Clash Of Clans</td>
</tr>
<tr>
<td>Leaderboards</td>
</tr>
<tr>
<td>Top 20</td>
</tr>
<tr>
<td>Best Student</td>
</tr>
</tbody>
</table>

Create a two point system:

**Smart points** can be spent at our online store for swag that interests the player.

**Trust points** are an aggregate of all the points you’ve earned over your lifetime.
Incentives gone wrong
Choose your key behaviors carefully
Incident Detection Results

- Salesforce employees trained to report *any* suspicious activity
- Customer reports also welcome

“My browser proxy settings were changed."

“Someone just badge surfed in our main floor.”

“I lost my sweater on the subway.”

“Is this email really from American Express?”
Connecting it to Social

Social Frontier — Emily

I got an email from info@supportforce-desk.com asking me to update my RSA token immediately because of a systemwide upgrade. I'm a little skeptical, not only because the message uses "do" for "due" (red flag for a writer!), misspells "inconvenience," and uses only my login name, but also because I just updated my token not long ago. Is this a security test or a legit request? I'm guessing the former. ... More

Comment · Like · Share · Yesterday at 10:20 AM

Devanshu Patel, Ed Mengel, and 2 others like this.

Christopher

Forward to security@salesforce.com anytime you get something that smells phishy like this one

Like · 1 person · Yesterday at 10:25 AM

Adam

Hey @Emily

Use this site - https://sites.google.com/a/salesforce.com/csitreport?pli=1 to report the email. They are pretty quick to get back to you to let you know if it's legit or not.

@Security

Like · 1 person · Yesterday at 10:26 AM

Emily

Thanks very much, Christopher and Adam. I'll send this to Security to see what's up.

Like · 1 person · Yesterday at 10:27 AM
Takeaways

Gamification: applying game mechanics to business

- Tap into discretionary performance

Steps to build your program:

1) Identify your key behaviors that you want to gamify
   - Prioritize them
   - Make sure gamification is the right approach to address the root cause

2) Communicate the expected behaviors to your employees.
   - What you want them to do and why

3) Reward/recognize people for the right behaviors when they do them
   - Measure it! Share it! Do it again!
thank you