Surfing the motivation wave to create security behavior change

Masha Sedova
Masha@ElevateSecurity.com
Elevate Security
About Me

Computer security meets behavioral science

Built and ran Salesforce trust engagement team

Passionate about transforming security behaviors from “have to” to “want to”

Co-Founder of security behavior change company
“I want my employees to be better at security”

This presentation will explore:

- Myths about influencing security habits
- The behavioral elements of human beings that can get us to security behavior change
- Focus on motivation as a key element
Myth #1

Training will change behavior
Historically, the industry solution has been to insist on terrible “check the box” trainings as an employee’s only defense.

95% of breaches are caused by human factors.

15% Retention
Rethinking Communications

The problem must be in the method of delivering this information - right?! We’ve been creative about ways to get information in front of people:

- Videos
- Posters
- Newsletters
- Websites
- Talks
- Lavatories

36.5 million adults in the United States currently smoke cigarettes
Knowing Isn’t Enough

WE UNDERSTAND WHAT GOOD PASSWORD BEHAVIOR SHOULD LOOK LIKE

- 59% know a secure password is important
- 91% understand the risk of reusing passwords

YET WE CONTINUE TO EXHIBIT POOR PASSWORD HABITS

- 41% choose a password that is easy to remember
- 61% use the same or similar passwords

Lastpass 2017
Behavior Change Components

- Motivation
- Ability
- Triggers
Behavior Change Model

By Dr. Bj Fogg
Myth #2

People have to care about security, all the time
Unrealistic Expectations
Security Action Can Be Simplified

**Having secure passwords for all sites**
- Remember 20 unique characters across 40+ sites

**Reporting suspicious activity**
- Look up correct email, reporting guidelines & send

**Stop tailgating**
- Social Accountability
- Install a man-trap or in/out badging

**HARD**
- Install a password manager

**EASY**
What about things that are hard to do?

By Dr. Bj Fogg
When Does Motivation Occur?

Hard things require high motivation.
Naturally Occurring Motivation

Predictable Events
- Audits
- Red Team exercises

Unpredictable Events
- Breaches
- Incidents
- News events
Good leaders seizes crises to remake organizational habits.

Charles Duhigg, The Power Of Habit
Myth #3

Money is a good motivator
Market Norms
Assigning a monetary value to an exchange

Social Norms
The actions among friends that are not based on money.

Dan Ariely, PhD
Predictably Irrational
“Generating” Motivation

- Connect security to the things people already care about.
- People are motivated by:
  - Hope/Fear
  - Social Acceptance/Rejection
  - Pleasure/Pain

Extrinsic | Intrinsic
---|---
Praise Punishment | Money
Interest Achievement
Punishment | Curiosity

People will do something because they matter, they are interesting, part of something more important.

*Daniel Pink, Drive*
Myth #4

Shame/blame for bad behaviors is a good tactic
Positive vs Negative Motivation

5:1 Positive to Negative exchanges

20% Of security teams have positive recognition programs
How to Create Positive Motivation

**Status**
- Leaderboards
- Top performer award

**Competition**
- Capture the Flag
- Bug Bounties

**Altruism**
- Feedback on their impact
- Champion Programs

**Access**
- Awarded points
- Access to exclusive swag

**Achievement**
- Recognition emails
- Company-wide shoutouts
Takeaways

- Motivation is required when something is hard to do.
- First- make it easy. Second- rely on motivation.
- Leverage naturally occurring events for motivation.
- Connect intrinsic motivations to security motivation.
- Negative feedback should be balanced with positive motivation.
Comments? Questions?

Let’s stay in touch!
@modMasha
Masha@elevatesecurity.com