KB4-CON

The Art and Science of Secure Behavior

Perry Carpenter, MSIA, C|CISO
Chief Evangelist & Strategy Officer

KnowBe4

KnowBe4

Security Awareness and *Secure Behavior* are NOT the Same Thing

Traditional awareness programs fail to account for the *knowledge-intention-behavior gap*

Agenda

1. Why behavior?
2. How can you model and design secure behaviors to help shape good security hygiene?
3. How can you debug behavior?

Agenda

1. Why behavior?
2. How can you model and design secure behaviors to help shape good security hygiene?
3. How can you debug behavior?

There are Three Realities of Security Awareness

1. Just because I'm **aware** doesn't mean that I **care**.

2. If you try to work **against** human nature, you will **fail**.

3. What your employees **do** is way more important than what they **know**.

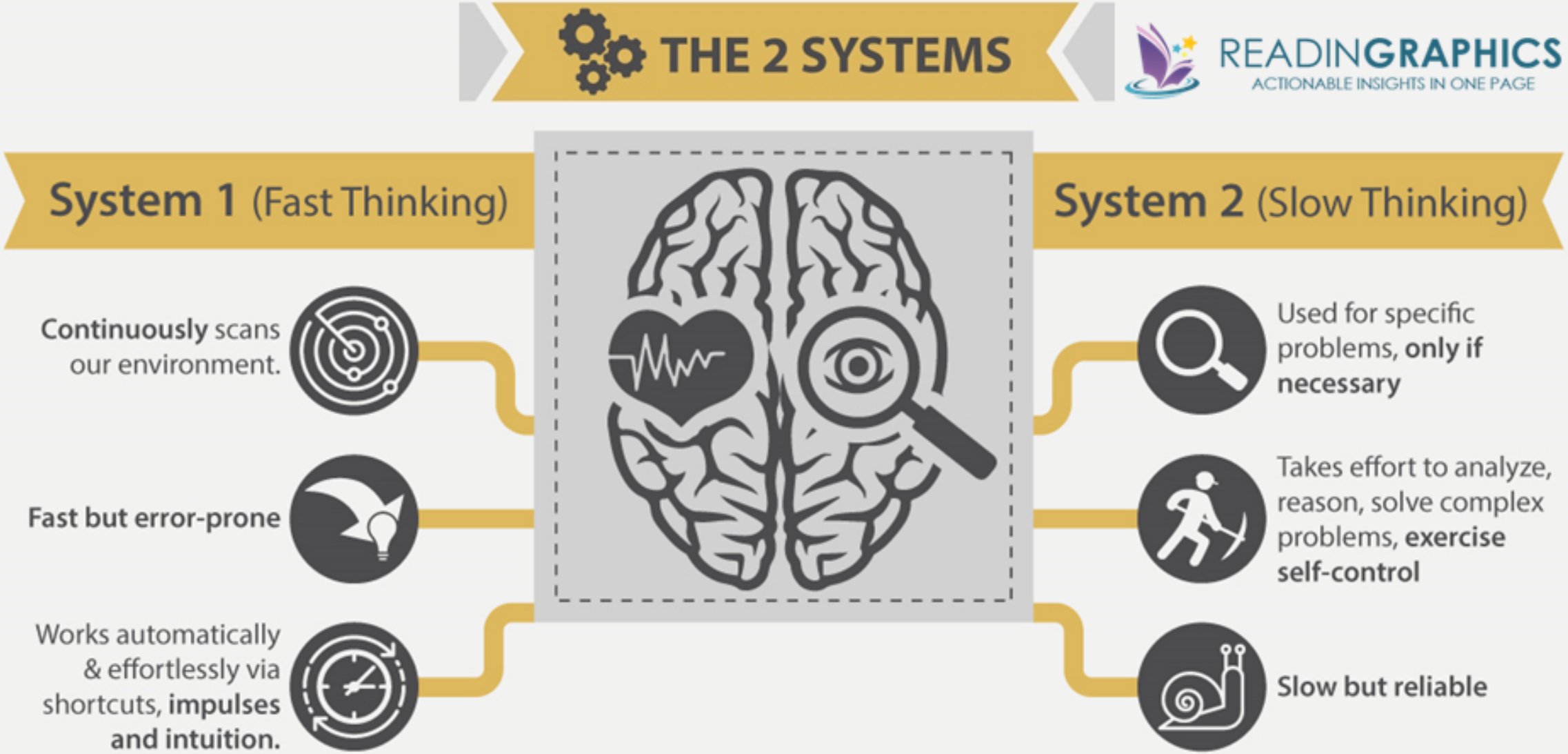
Security Awareness and *Secure Behavior* are NOT the Same Thing

Just because I'm *aware* doesn't mean that I *care*.

If you try to work against human nature,

you will fail…

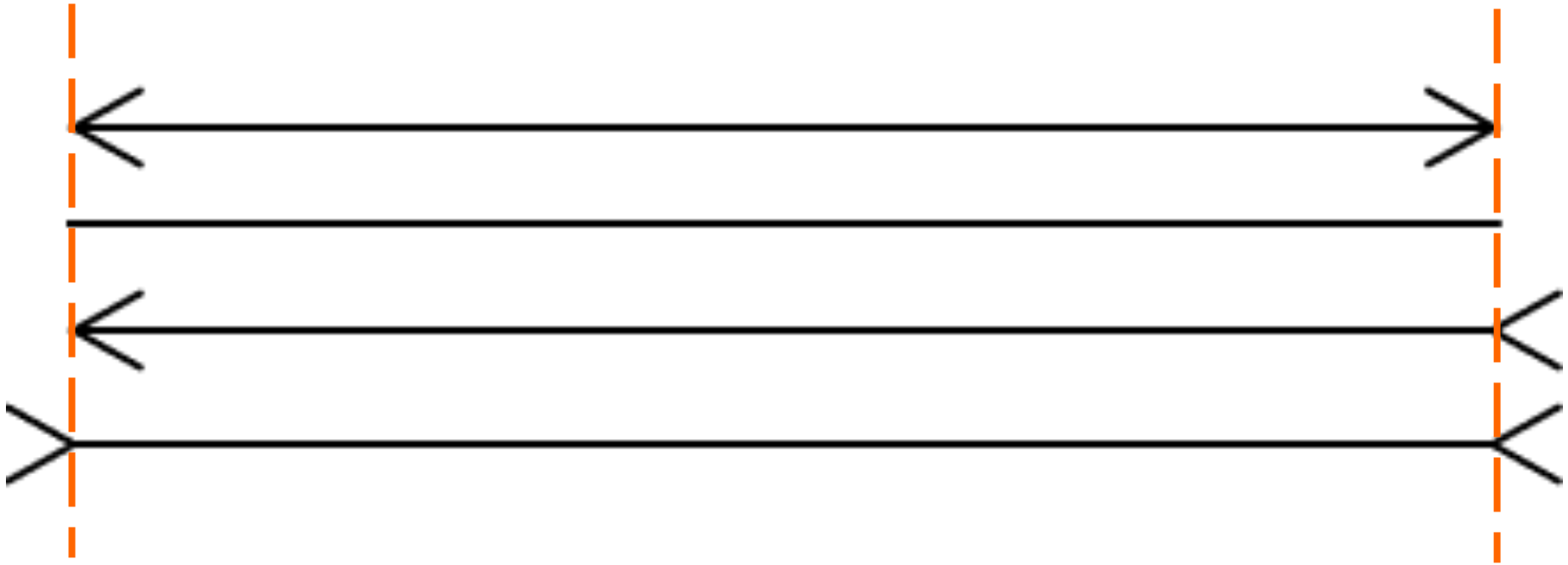
Thinking, Fast & Slow (Daniel Kahneman)



Graphic Source: https://readingraphics.com/book-summary-thinking-fast-and-slow/

System 1 Thinking Example

Which line is longest?



System 2 Thinking Example

Solve for *x*:

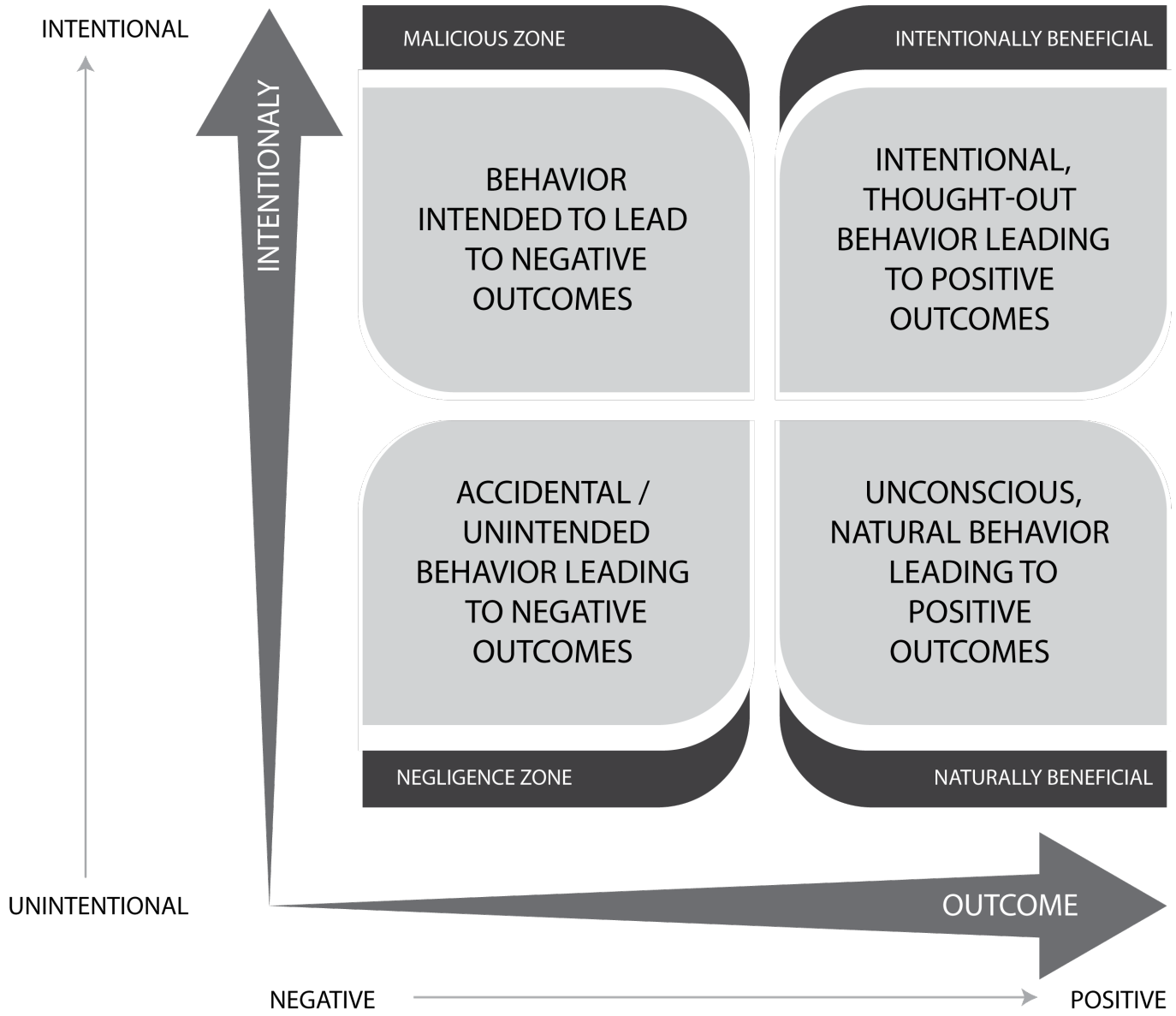
532 ÷ 86 = *x*

Your awareness program should not focus only on information delivery

Ask yourself:

Do you care more about what your people ***know*** *or what they* ***do****?*

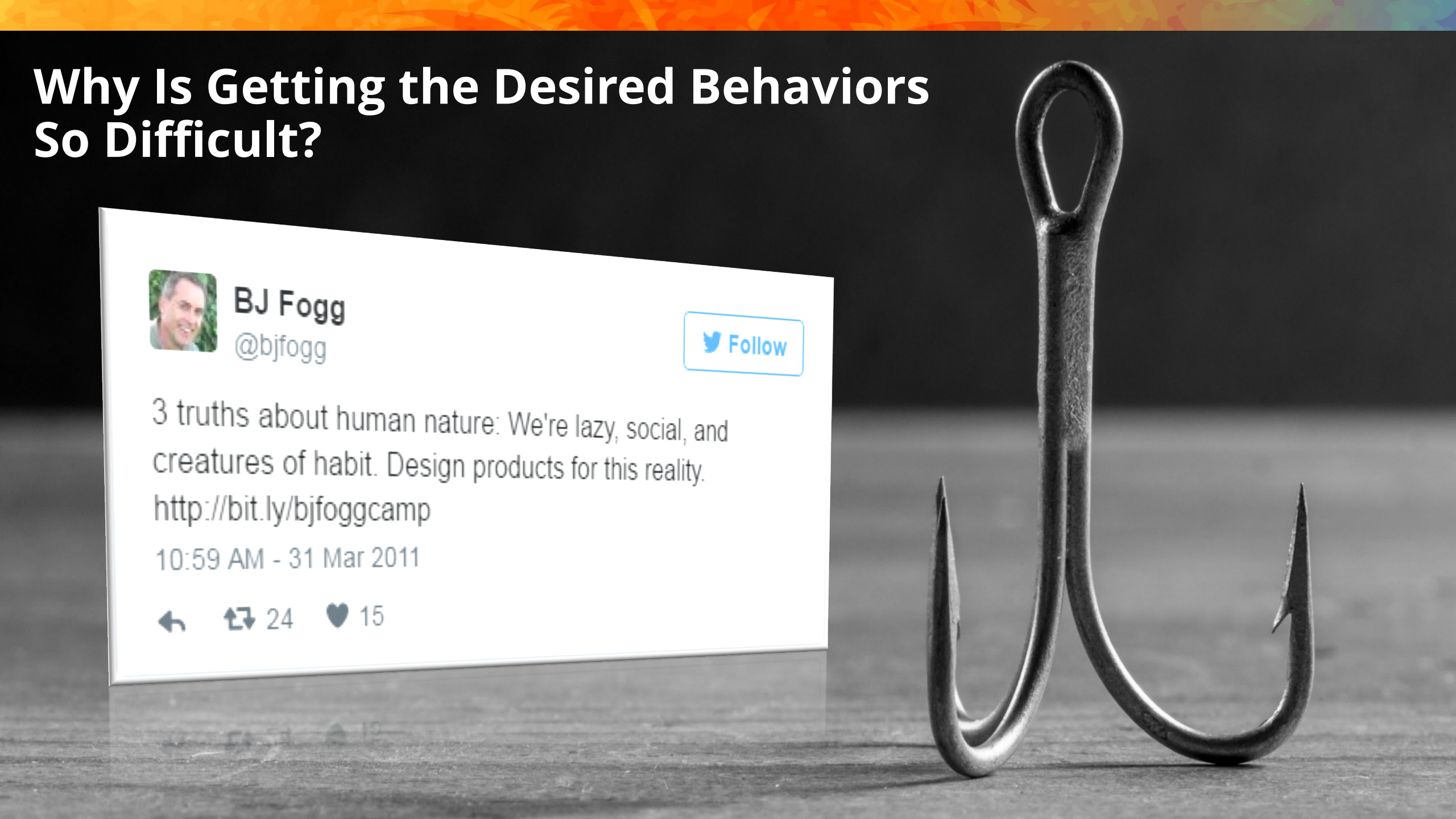
Thinking about Behavioral Intersections and Interventions



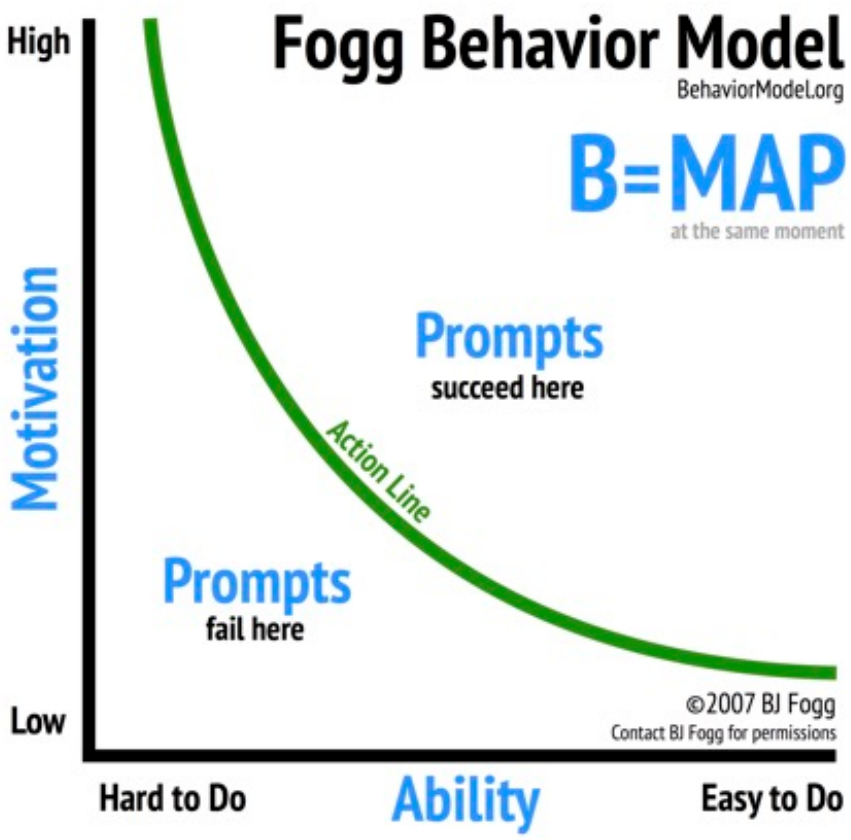
Agenda

1. Why behavior?
2. How can you model and design secure behaviors to help shape good security hygiene?
3. How can you debug behavior?

Why Is Getting the Desired Behaviors So Difficult?



BJ Fogg** is the father of a field now referred as **"Behavior Design."



http://behaviormodel.org

Behavior happens when three things come together at the same time:

Motivation, ***Ability***, and a ***Prompt*** to do the behavior…

Get Specific:

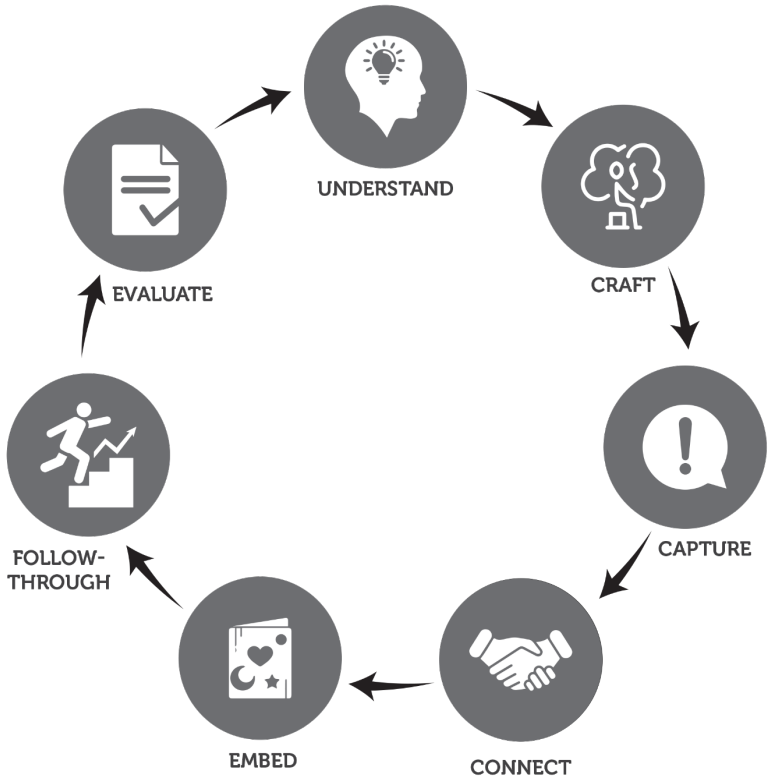
1. What behaviors, if adopted, would have the most security benefit for our organization?
2. Is this a group of behaviors, or is this a single behavior?
3. Is this a behavior that we have the appetite to take-on right now?

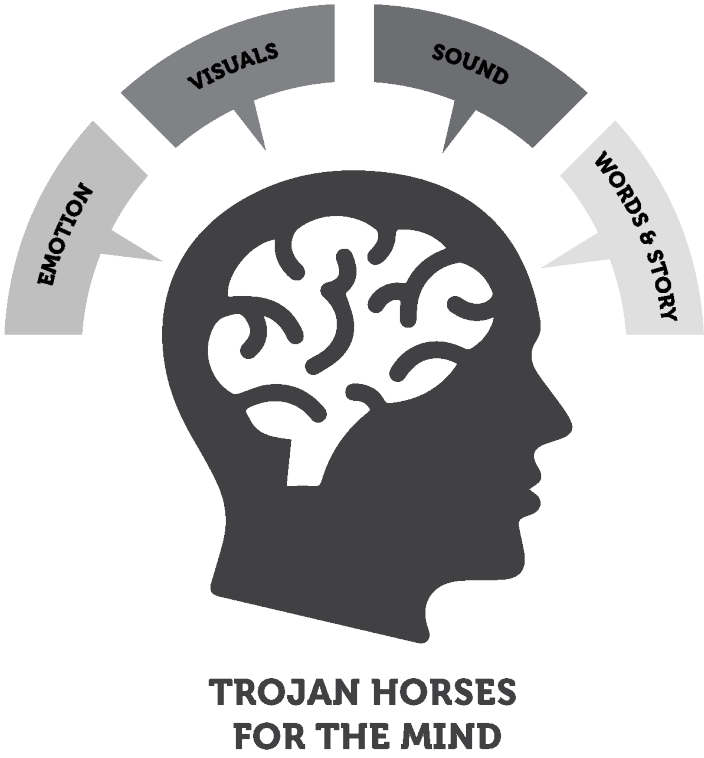
Designing Behavior (A Non-Security Example)

Fogg Behavior Model Component	Description
Behavior(B): What specific behavior do we want someone to do?	Drink a glass of water
Motivation(M): What types of things might motivate someone to perform the B?	• They could be thirsty • The might want social acceptance (everyone else is doing it) • They might want to avoid offending the person offering them water • They believe that there are positive health benefits associated with staying hydrated • Etc.
Ability(A): What types of things must someone already be able to do or know to successfully perform the B?	• A glass of water is available to the person or can be obtained with little effort • The person's mouth is not taped shut • The person is not asleep or otherwise incapacitated • Etc…
Prompts(P): What types of things can cue the B?	• The person noticing that they are thirsty • Someone offers the person a glass of water • The person receives a prompt from a health-app reminding them to drink • Etc.

Thoughts on Designing for Each Element

- Prompts
- Ability
- Motivation





Learn from Marketers and Storytellers to Influence Motivation

Nudge your audience toward the behavior

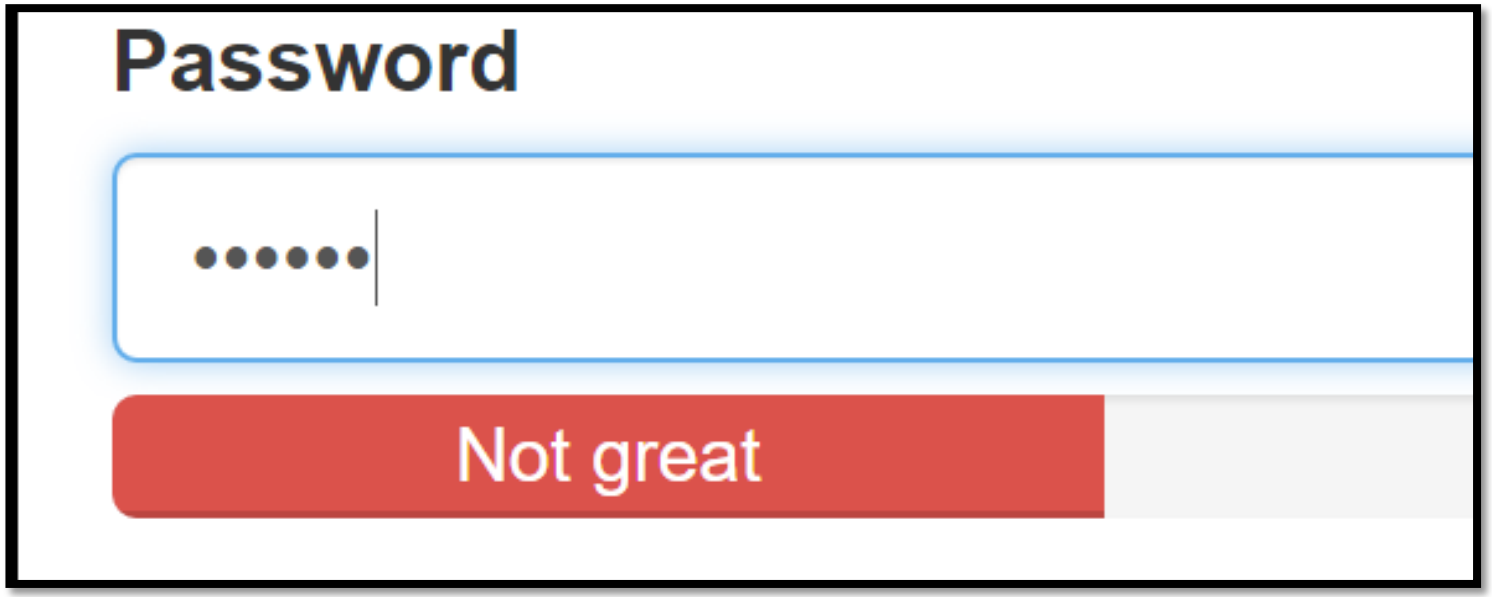
A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not.

Nudge: Improving Decisions About Health, Wealth, and Happiness, 2008

Nudge them in the right direction

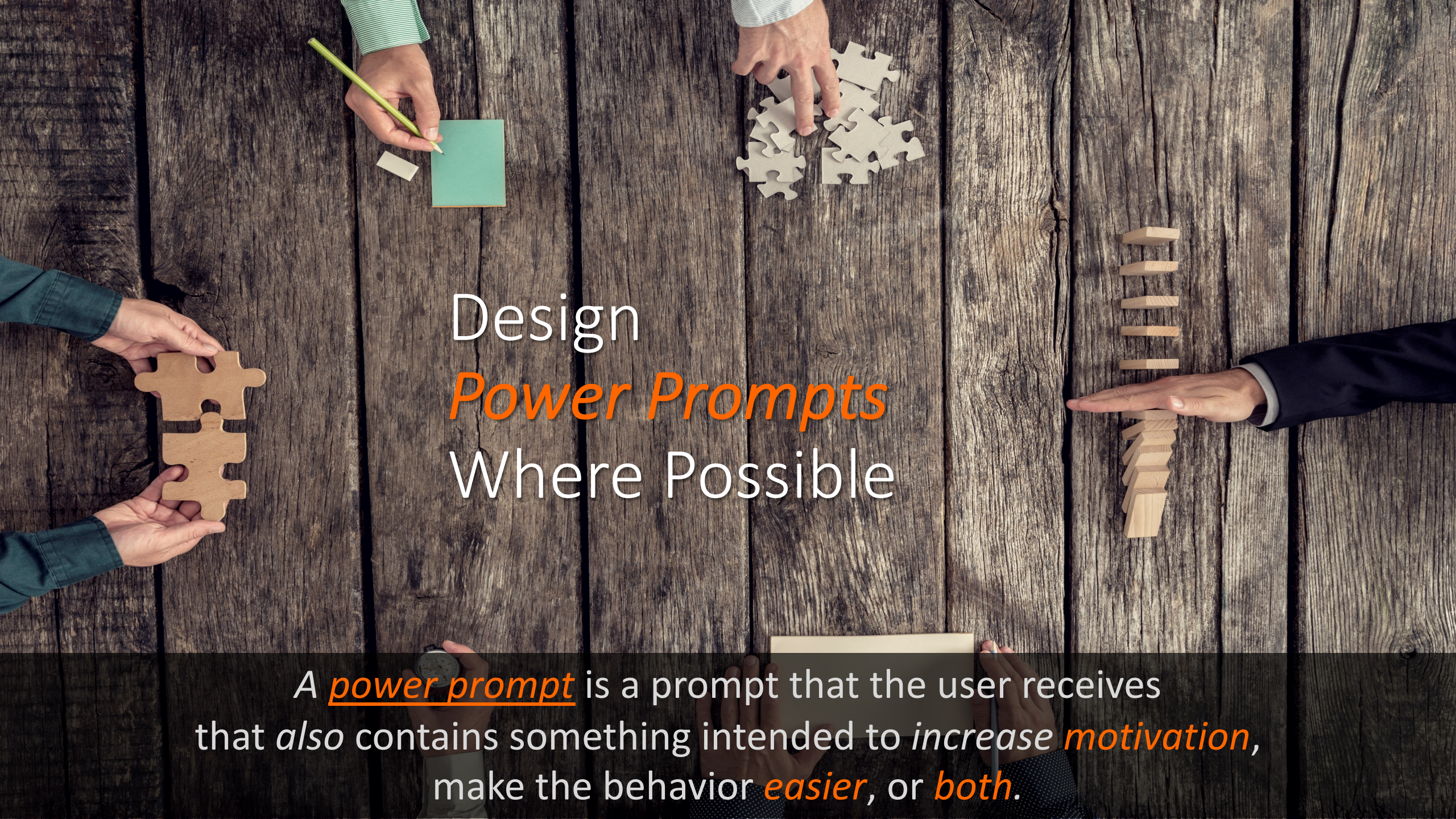
A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not.

Nudge: Improving Decisions About Health, Wealth, and Happiness, 2008



Your password change portal is a great place to insert a nudge:

- Strength Meters
- Videos on how to create & remember strong passwords
- Elective LMS modules
- etc.



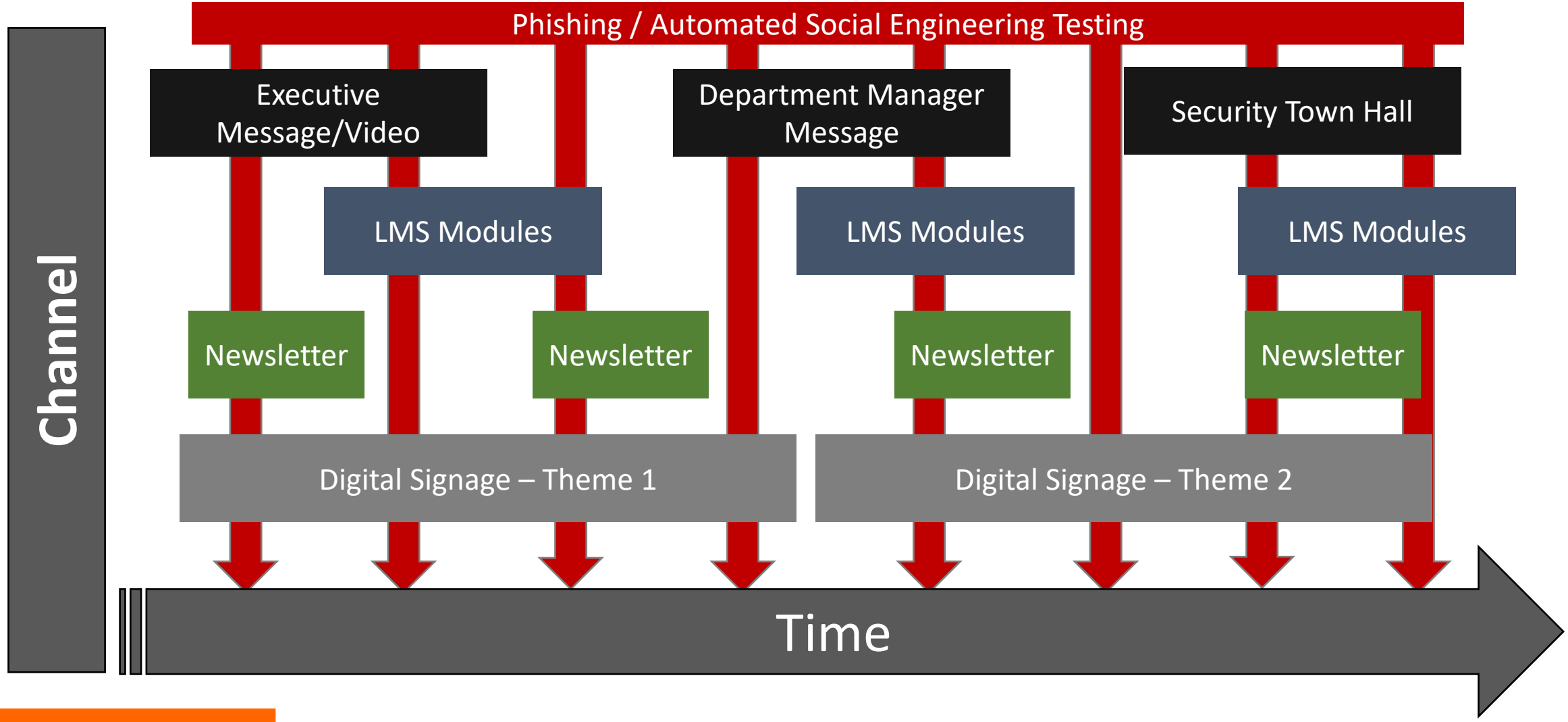
Design *Power Prompts* Where Possible

A power prompt is a prompt that the user receives that *also* contains something intended to *increase motivation*, make the behavior *easier*, or *both*.

Designing Behavior (A Security Example)

Fogg Behavior Model Component	Description
Behavior(B): What specific behavior do we want someone to do?	Choose a good password
Motivation(M): What types of things might motivate someone to perform the B?	• They understand and appreciate the value of choosing a good password • They feel empowered by choosing a good password • They feel more secure by choosing a good password • They are afraid that their current password has been (or might be) compromised due to its simplicity • They feel pressure to create a better password because the organization is monitoring password strength
Ability(A): What types of things must someone already be able to do or know to successfully perform the B?	• The person has the required knowledge of how to construct a password that is both strong and memorable • The person has tools that will help them construct a password that is both strong and memorable • The person has tools that will choose a strong password and remember that password for them
Prompts(P): What types of things can cue the B?	• The person just feels like changing their password • The person receives notification that it is time to change his/her password • The person is locked-out of his/her account because they forgot their current password • The organization issues a forced password reset • The person receives a security tip that has advice on how to create and remember a good password • The person forgot their current password and is about to perform a password reset • The person receives a notification that his/her account was breached, and hackers may have accessed the password

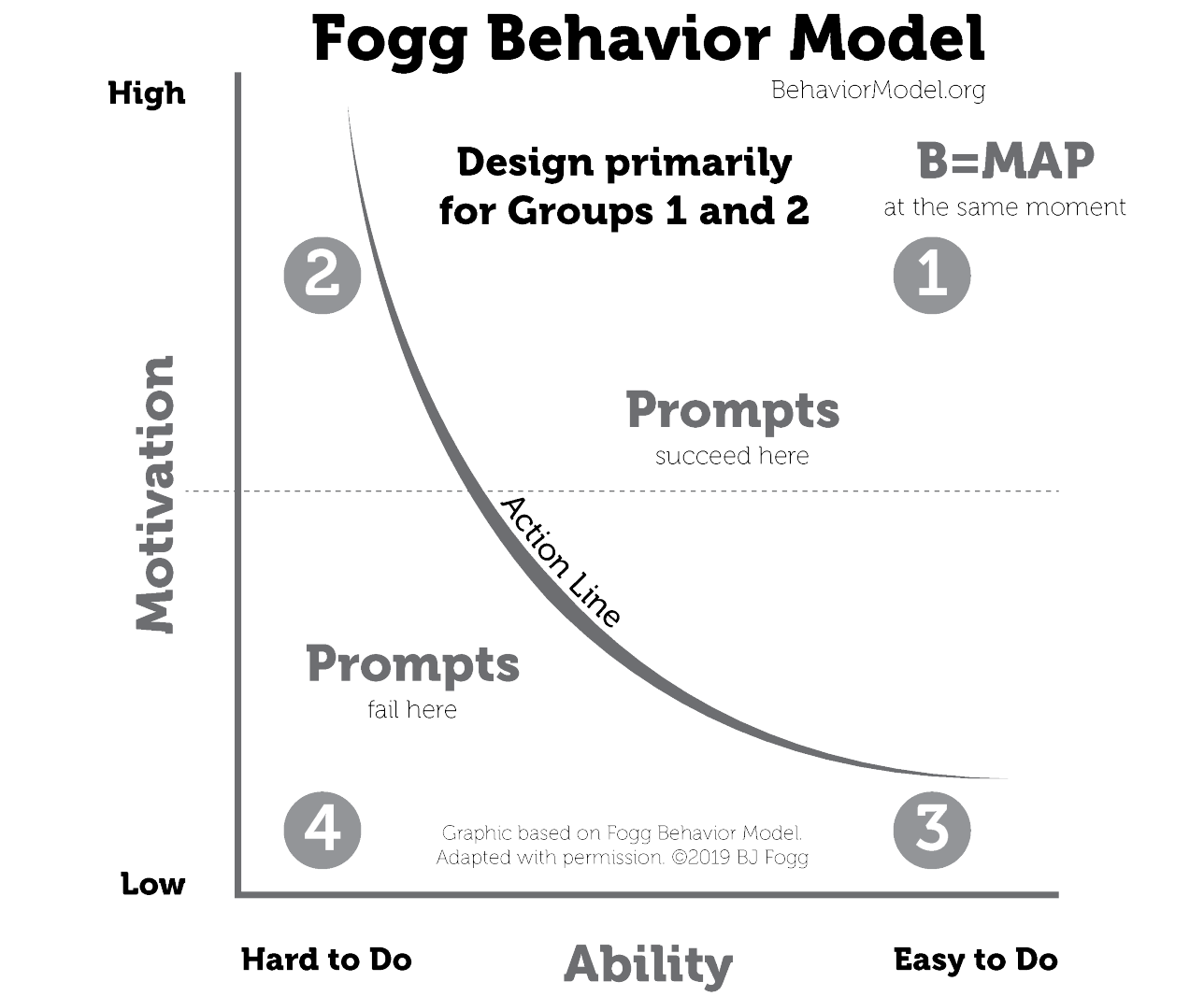
Plan like a Marketer. Test like an Attacker.



Agenda

1. Why behavior?
2. How can you model and design secure behaviors to help shape good security hygiene?
3. How can you debug behavior?

Account for Behavioral Segments



Debugging Problem Behaviors

Prompt:

- Are we prompting for the behavior? If not, prompt for the behavior.
- If so, are the prompts designed effectively?
- Have the prompts become ‘invisible’ through overuse?
- Are the prompts occurring through an optimal channel?
- Can we create a power prompt?

Ability:

- Is the behavior still too hard?
- Is there any way to make the behavior easier? Perhaps through tools, additional training, etc.?
- Is this behavior even something most humans can do consistently?
- Is there a time that the behavior feels easier or more achievable than other times?
- Can we embed something within the prompt that will reduce the real (or perceived) time, complexity, or effort required to do the behavior?

Motivation:

- What factors might enhance or erode emotion at the time of behavior?
- Are their times when someone may feel more naturally motivated to do the behavior?
- Is there a way to make the behavior feel more meaningful?
- Are their social, environmental, or other factors that can be leveraged to provide intrinsic or extrinsic motivation?
- Can we place a motivational boost within the prompt?

Designing for the Larger Issue

thinking about passwords

Thank You!

Perry Carpenter
Chief Evangelist & Strategy Officer

KnowBe4

KnowBe4