

# Information Security Nudges

Chris Walsh - [chris@cwalth.org](mailto:chris@cwalth.org)

# It would be nice to...

Design systems with an awareness of human cognitive limitations and biases.

Allow decision-makers (“users”, customers, etc.) to make sensible security-relevant choices.

Allow organizations to guide behavior in “secure directions”, rather than resorting to stifling coercion.

Do the above in a manner allowing for quantitative assessment.

# “Cognitive limitations and biases”?

**Framing effect** Drawing different conclusions from the same information, depending on how that information is presented.

**Hyperbolic discounting** The tendency for people to have a stronger preference for more immediate payoffs relative to later payoffs, where the tendency increases the closer to the present both payoffs are.

**Loss Aversion** Stronger preference to keep something than to obtain it in the first place.

**Confirmation bias** The tendency to search for or interpret information in a way that confirms one's preconceptions.

# So what?

Information security is very much a social science

- The product of human will
- We set systems up certain ways
- We design screens in certain ways
- We choose defaults

It is also an area *rife* with poor choices

Thus (says I) information security is an area in which understanding and influencing human decision-making can lead to real improvement

*Choice architecture* describes organizing the context within which decisions are made. When a choice architect influences decisions through her design of the context in which they are made, she is said to provide a "nudge".

# Examples

- Organ donor opt-out versus opt-in
- Default 401k allocations
- “Discount for cash”
- Other interesting applications

Which city do you live in?



San Francisco, California



Susan lives here.

I live here

Choose another city

# Why I am here

Brainstorming about possible infosec nudges, eg.:

- Impact of defaults
- password strength indicators, rewards
- general incentive alignment through carrot more than stick

What else?

How can we test? Can we test?