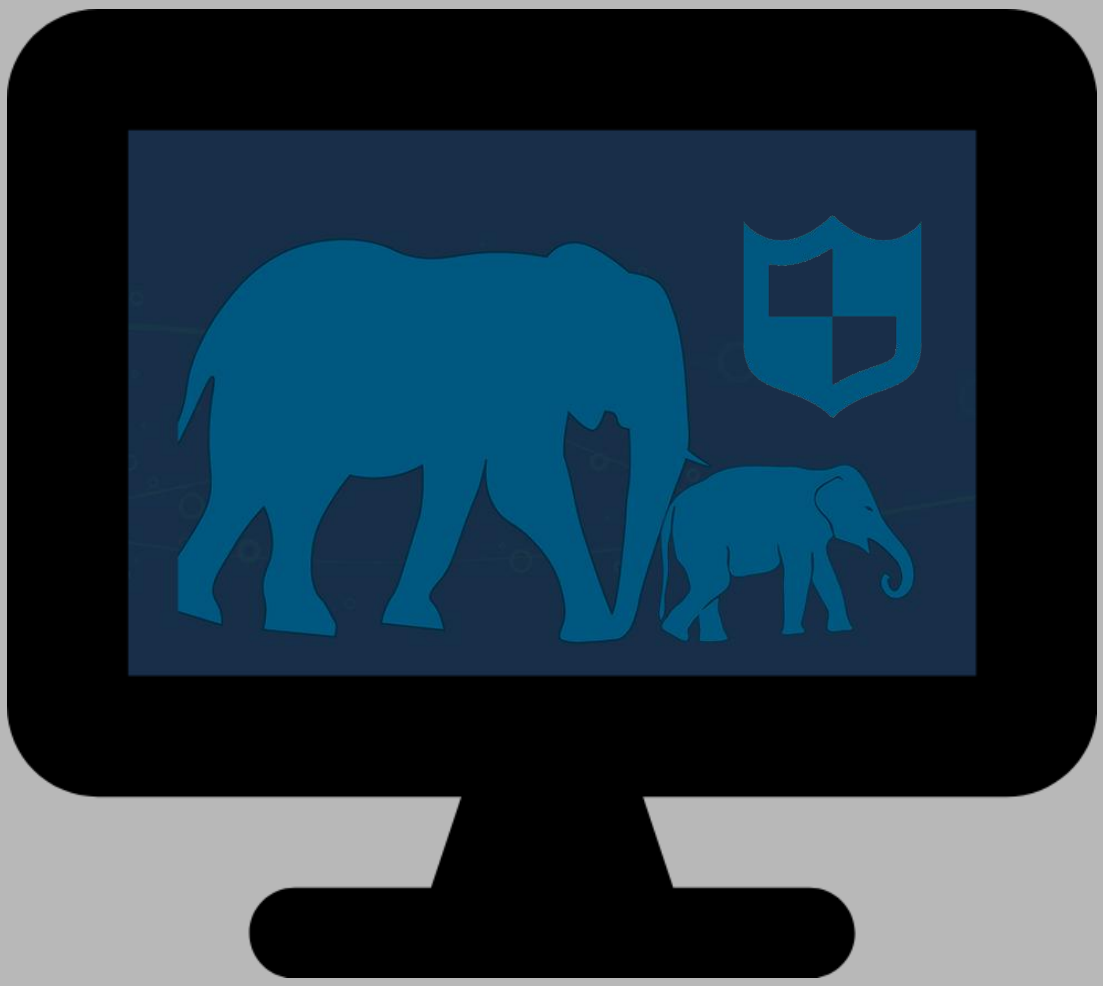
DAYBLINK



Nudging for Cybersecurity

July 2019

By Clare Suter

With contributions from Jacob Armijo, Justin Whitaker, and Michael Morgenstern

INTRODUCTION

Why do security awareness trainings fail to impact employee behavior, and how can *nudging* help?

All too often, cybersecurity is perceived to be overwhelmingly technical in nature. However, Information Security professionals would be wise to keep in mind the words of security expert and cryptographer Bruce Schneier: "Only amateurs attack machines, professionals attack people". Security infrastructures can be intricate and robust, but a careless employee can easily render these painstaking defense mechanisms meaningless by failing to take simple precautions. Though security awareness trainings are commonly held in order to train employees in best practices, a substantial body of research indicates that knowledge of how to protect oneself does very little to translate into safe security behavior.[1]

Approximately 90% of all cyber claims are the result of some type of human error or behavior.[2]

Thus, organizations are left vulnerable not due to immature security infrastructures, nor to lack of awareness surrounding cybersecurity threats and proper precautions, but to employee behavior which is consistently and irrationally counterproductive to desired outcomes. For example, many employees are well aware that the comfort enjoyed when choosing not to increase the complexity or diversity of their passwords is far overshadowed by the costs associated with the exposure to cyber risk that derives from lazy password practices. They don't want their company exposed to a cyber attack, and they certainly do not want the origins of such an attack to be traced back to their personal security habits. Yet, they keep the simple, convenient passwords anyways. Any solution hoping to bridge the gap between knowledge of security policy and subsequent action requires an understanding of the behavioral factors that drive irrational decision-making and cause well-intentioned employees to neglect their security responsibilities.

[1]Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices: A Rational Choice Perspective." Journal of Organizational and End User Computing (16:3), 22-40.
[2]"When It Comes to Cyber Risk, Businesses Are Missing the Human Touch." *Willis Towers Watson*, 2 Mar. 2017, www.willistowerswatson.com/en-US/news/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch.

Luckily enough, insights from the rapidly growing field of behavioral economics have proven that such departures from rationality are predictable. Therefore, given a knowledge of the mental mechanisms that lead to poor choices, decisions can be strategically redesigned in order to promote (or "***nudge***" people toward) a desired behavior. In other words, nudges give organizations the power to leverage the predictability of cognitive biases and heuristics alter the decision landscape in a way that results in better outcomes without actually restricting employee agency.

Nudge: **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**[3]

Nudges in Practice

At first, nudging as a significant force of change may seem too good to be true. How could policy lacking overt direction or compulsion drive behavioral transformation on a large scale? As it turns out, results from nudge-inspired interventions around the world seem to speak for themselves.

- Employers who enrolled employees automatically in retirement savings plan, while providing the option to opt out saw plan participation rates of **91%**, compared to rates of 42% from employers whose default option was no enrollment[4]
- After the image of a fly was etched near the drain in the Amsterdam bathroom urinals, subconscious "aiming" ensued, and spillage on the floor was reduced by **80**%[5]
- On Lake Shore Drive in Chicago, a certain curve became notorious for accidents, as it was sharp, and frequently taken too fast by drivers. The city repainted the lines to give the illusion that drivers are going faster than they actually are, causing them to slow down in response. In the next six months, there were **36%** fewer crashes on that curve[6]
- Customers at a grocery store were given a cart with duct tape on the bottom of the cart. They were then handed out flyers instructing them to put fruits and vegetables on one side of the tapeline, and everything else on the other. A **102%** increase in fruits and vegetables resulted[7]
- In the United Kingdom, people in arrears on their taxes were sent flyers detailing information about the tax compliance of their neighbors, such as "9 out of 10 people in your area paid their taxes on time. Tax payments from these people subsequently increased by **15%**[7]

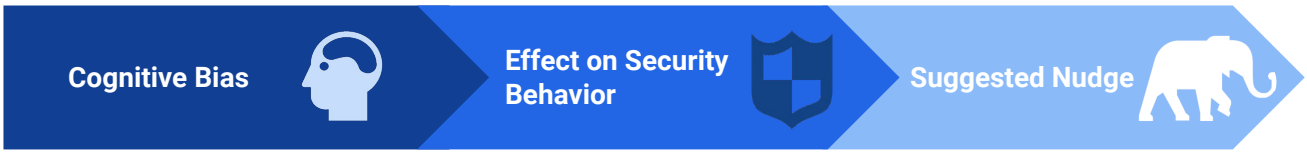
[3]Thaler, Richard H., and Cass R. Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin, 2009, 6.
[4]Salisbury, Ian. "Meet Richard Thaler, the Man Who Just Won the Nobel Prize for Helping You Save for Retirement." *Money*, 9 Oct. 2017, money.com/money/4974462/thaler-nobel-economist-retirement-savings-nudge/.
[5]Krulwich, Robert. "There's A Fly In My Urinal." *NPR*, NPR, 19 Dec. 2009, www.npr.org/templates/story/story.php?storyId=121310977.
[6]"Measuring the LSD Effect: 36 Percent Improvement." *Nudges.org*, 11 Jan. 2010, nudges.org/?s=lake%2Bshore%2Bdrive.
[7]Clarke, Marcus. "Infographic: 10 Amazing Examples of Nudge Theory." *Global Applied Ethics Institute*, 26 Apr. 2018, gaei.org/nudgetheory/.

Nudging has been found to be so successful and cost-effective that several countries such as Japan, Germany, and the United Kingdom have recently established "nudge units" within their governments to improve decision-making by changing the choice architectures faced by their citizens. Given the human-centric nature of today's cyber attacks, thoughtfully employed nudges display promise of closing the gap between security policy and compliance, and of minimizing organizational cyber risk where many other methods have failed.

CREATING NUDGES FOR CYBER

Creating nudges specifically designed to improve employee's security behavior requires an understanding of how biases disrupt rational decision making when people make choices such as whether or not to perform a suggested system update, or adopt multi factor authentication. In this guide, the relevant behavioral science concept will be introduced, followed by an explanation of how this concept dictates behavior in a certain security-sensitive setting. Once the cognitive processes operating behind current decision-making are identified, a nudge is suggested which will work to correct for biases, and align employee choices with security-friendly behavior.

Nudge #1: The Affect Heuristic and Risk Assessments



The **affect heuristic** is a reliance on good or bad feelings experienced in relation to a stimulus. It involves quick, automatic thinking, and is rooted in visceral emotional reactions rather than calculated judgement.[8]

An employee wants to watch his favorite team play in a championship, but he can't find a way to stream the game other than via an illegal website. To decide whether to use the illegal site, he uses the **positive emotions** associated with watching his team play, rather than a consideration of the risk of acquiring a virus.[9] How could being able to watch the game be a bad thing?

Install pop-ups on sites that are known to play host to viruses, with a reminder that serves to concretize risks, and make potential costs more salient. Also, consider conveying information about malware consequences via browser warnings or search results.[9] This will present the user with the information he should be using to make such a decision, and will serve to **mitigate the role of emotion** relative to that of factual risk.

[8]"Affect Heuristic: Behavioraleconomics.com: The BE Hub." *Behavioraleconomics.com | The BE Hub*, www.behavioraleconomics.com/resources/mini-encyclopedia-of-be/affect-heuristic/.
[9]Blau, Alex, et al. "Deep Thought: A Cybersecurity Story." *ideas42*, Aug. 2016, www.ideas42.org/wp-content/uploads/2016/08/Deep-Thought-A-Cybersecurity-Story.pdf, 19.

Nudge #2: Habituation and Security Warnings

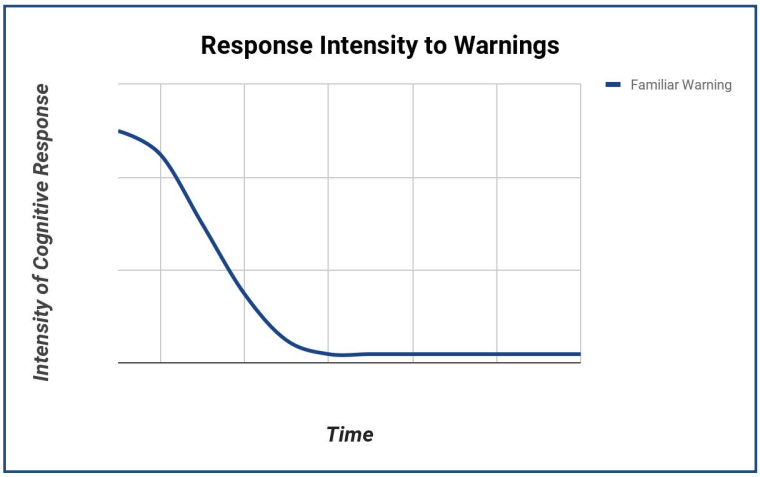
Cognitive Bias | **Effect on Security Behavior** | **Suggested Nudge**

When people are repeatedly exposed to the same stimulus, their reaction becomes significantly diminished through a process called **habituation**.

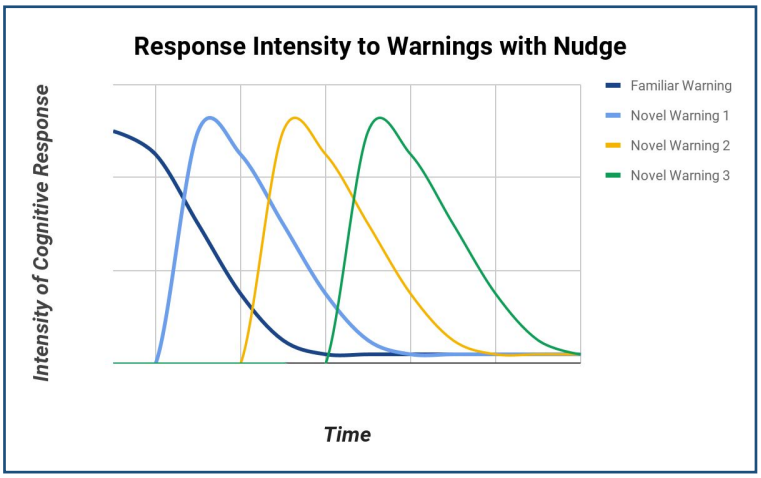
Most security warning messages are similarly designed, and users are often exposed to several on a daily basis. They become habituated to the warnings, which causes them to **click through automatically**, often without reading a single word of the notification, and certainly not heeding any request made.

To attract user attention and improve adherence to warning messages, build warnings that **are characterized by unfamiliar UI features** and require the user to complete various types of actions in order to click through. For example, polymorphic, or color-changing warnings have been documented as successfully improving adherence.[10]

Habituation Nudge: *Visualized*



Assuming fairly regular frequency of exposure, the longer a user has seen the same type of security warning, the smaller the user's cognitive response to each warning. Finally, when a user has become used to these security warnings, the intensity of their cognitive response essentially stalls at a level that represents the user barely registering the warning. For some, the response intensity can level off at its minimum after only a few weeks of working on a computer.



*When the presentation of warnings to the user is changed, each individual presentation is still subject to habituation and diminished cognitive response over time. Importantly though, the user's cognitive processes register each significantly different presentation as a **novel phenomenon**, even if the content has not changed. Thus, **intensity of response can be revived**, (and retained if warnings are changed often enough). In this chart, the peak of each warning represents its initial introduction to the user.*

[10]Blau, "Deep Thought: A Cybersecurity Story.", 22.

Nudge #3: Hyperbolic Discounting and Updates

Cognitive Bias | **Effect on Security Behavior** | **Suggested Nudge**

Hyperbolic discounting refers to the tendency of people to increasingly choose a smaller reward sooner, rather than a larger reward later.[11] It is the same bias that contributes to common errors such as not saving enough for retirement, as well as poor dietary and exercise choices.

When notifications concerning software updates appear, they are often accompanied by a choice of completing the update now, or later. Choosing to push the update to "later" brings the **instant** reward of continuing to use one's computer freely. Choosing "now" means greater protection against a possible security threat that is almost certainly not imminent, but would occur **at some unknown point in the future.** Though the cost of a security breach (even taking into account low probability of a breach) would certainly exceed the reward of continued work that comes with declining the instant update, people consistently choose to neglect updates.

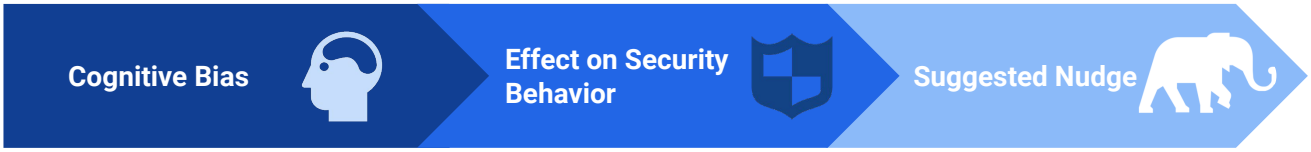
To make costs of neglecting a patch more salient and reduce the degree to which the non-instant reward is discounted, provide **information about the purpose** of the patch.[12] Additionally, managers can help their employees **make a commitment** to update by having an administrator send an email instructing employees to block off a time on their calendar to complete the update.[13] Beyond providing a clear reminder and source of guilt, blocking off time for the patch will reduce the probability that other computer activities sensibly take precedence or compete for immediate reward.

More on Hyperbolic Discounting:

It may appear that people fall victim to hyperbolic discounting because the payoffs in separate periods aren't always comparable, such as in the choice between getting to continue working on a time-sensitive project, or protecting oneself against cyber attacks that might come at some unknown point in the future. However, research has demonstrated the striking pervasiveness of hyperbolic discounting in scenarios in which the more immediate reward is quite obviously inferior to the delayed reward. Even when given the choice between $100 now and $120 in a week, adults and children alike will consistently choose the $100 now in a way that contradicts their incentives to maximize payoffs from any given choice.[14]

[11]www.behaviorlab.org/Papers/Hyperbolic.pdf
[12]Blau, "Deep Thought: A Cybersecurity Story.", 24.
[13]Blau, Alex. "Better Cybersecurity Starts with Fixing Your Employees' Bad Habits." *Harvard Business Review*, 11 Dec. 2017, hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits.
[14]Laibson, David. "Golden eggs and hyperbolic discounting." *The Quarterly Journal of Economics* 112.2 (1997): 443-478.

Nudge #4: Scarcity and Access Control Management



Behavioral science research has revealed that the **context of scarcity** introduces a psychological burden, and inhibits cognitive power. This happens because of a response to scarcity called "tunneling", in which people focus on the tasks or activities that are most pressing, which crowds out essentially everything else.[15] Tunneling is frequently induced by a shortage of time or money.

Access control management is a vital component of the information security practices of a modern workplace. Scarcity of time, which occurs frequently in workplace settings, causes managers who play a critical role in access control tasks to restrict their attention to urgent tasks that have nothing to do with access control management. It's far too easy to **repeatedly postpone the daily management of security controls.**

To substantially reduce the load placed on those in charge of access control management, **leverage defaults to automate part of their responsibilities**.[16] Changing the default to having permissions automatically expire after a certain time if not manually reviewed can spare managers a good deal of sanity. Now, they no longer face the stress of knowing that the longer they neglect the control management grind, risk, borne from their inability to keep up with access control work, is growing exponentially. Also, this default situation affords managers the ability to prioritize their work based on whose expired controls need review, rather than consistently assessing the validity of all existing permissions.

Nudge #5: The Congruence Heuristic and Risk Assessment

The **congruence heuristic** is a mental shortcut which occurs when someone tests a hypothesis by looking *only* for confirmatory information while simultaneously ignoring alternative hypotheses.[17]

The congruence heuristic is dangerous to security behavior in that it causes organizations and people alike to **under weigh the likelihood of a breach** simply because they haven't had one in the past. Their lack of experience with security breaches causes them to believe they aren't at a worrisome level of risk, and that they can expect an absence of breaches in the future, because it is all they've known.

Tools should be developed and used to help guide investment decisions in security resources in a way that prompts decision makers to consider alternative hypotheses (in this case, the real risk faced by the company of a security or privacy breach). In making these risks salient, decision makers should be **less inclined to use biased evidence, and make better investment decisions** reflecting the reality of an organization's security posture.[17]

[15]Mullainathan, Sendhil, and Eldar Shafir. *Scarcity: Why having too little means so much*. Macmillan, 2013, 30.
[16]Blau, "Deep Thought: A Cybersecurity Story.", 109.
[17]Blau, "Deep Thought: A Cybersecurity Story.", 51.

Nudge #6: Underestimating Predictability and Passwords

Cognitive Bias → **Effect on Security Behavior** → **Suggested Nudge**

People tend to be both **extremely predictable** in the way they choose to comply to bothersome rules, and **likely to underestimate their predictability and similarity to others** in their methods of compliance.[18]

The relatively new password requirements which demand a certain degree of complexity were meant to be applied to randomly generated passwords. However, the **average person's password is far from random**, and **so is the way they change their ideal password to reach compliance** with these requirements. For example, people will overwhelmingly satisfy the demand for a special character by adding an exclamation point at the end of their previous password, or will change an "a" to an "@". Predictable patterns such as this render complexity requirements close to useless, and in some cases, increase the likelihood that an account will be hacked.

Companies like Apple have begun providing users of their products with the option of selecting a randomly generated password to be saved and used for future logins on that device. Unfortunately, these passwords are nearly impossible to memorize. To promote both safely complex password adoption, and memory of the password so the user is comfortable and willing to adopt, suggest to users **randomly selected dictionary words** as the base of the password, while **incorporating special character or number placement that defy predictable tendencies** without being overwhelmingly complicated.[18]

Examples of Password Changes:

`@nnabelle7`	**Witwanton:** disrespectfully witty	`0%witWanton`
`NotreDame4Life!`	**Draconiform:** dragon-shaped	`9#Draconiform`
`Barcelona10!`	**Cynology:** the scientific study of dogs	`48Cynology*`

Password Length vs Complexity

*It is recognized that in order to achieve greater password entropy, length is often more critical than common complexity. However, complexity restrictions are more predictable in terms of user compliance, as well as more restrictive or taxing in passphrase formation than the typical 8 or 10 character character minimum. Assuming user unwillingness to go well beyond the minimum password requirements, a "nudge" to alter the way users comply to complexity demands is a fitting way to decrease predictability without doing more than is asked by minimum requirements. Ideally, passwords would also increase in length as well to ensure better security.**

[18]Blau, "Deep Thought: A Cybersecurity Story.", 33.

Nudge #7: Hassle Factors, Status Quo Bias, and MFA

Cognitive Bias | **Effect on Security Behavior** | **Suggested Nudge**

When people don't act in accordance with their intentions because of seemingly minor inconveniences, they are experiencing **hassle factors.** Often times, these are generated by annoyances associated with minor tasks, especially those that involve complex processes or unanticipated steps.[19] Also relevant in the following security scenario is the **status quo bias**, via which people exhibit a preference for the way things are currently. When changes do occur, they are often perceived as a loss or a detriment.[20] Sometimes, this bias comes from a tendency of inertia, or the relative ease of inaction.

In the context of **low adoption rates of multi-factor authentication (MFA) programs**, hassle factors have significant explanatory power. Users could be wary of the hassles associated with needing to use their phone or some other device to authenticate themselves, conjuring up scenarios in which they lack cell service or their phone is dead, and reinforcing the dramatic perception of hassles involved.[21] Additionally, the opt-in nature many of MFA systems paired with status-quo bias renders users even more unlikely to act against the default (no MFA enrollment), and brave associated hassles.

To see increases in MFA enrollment, **ensure that the default option is enrollment**, so that the "do nothing" tendency associated with status quo bias works *in favor* of MFA adoption rates. Furthermore, this opt-out scenario will create hassle factors surrounding the action of opting out, making people view it as prohibitively cumbersome, even if they remain somewhat concerned about MFA related inconveniences. If users are staunchly opposed to MFA, and wish to unenroll, they are free to do so. It is more likely, however, that hassle factors were irrationally preventing adoption, and once those are reversed, user desire for increased security will no longer be irrationally distorted by minor features of adoption.

Power of the Default:

- Though most people approve of organ donation, only a fraction of people actually enroll themselves as an organ donor when such a choice is "opt-in". 25 European countries took note of this, and changed the decision for their citizens to an "opt-out" design. By making donation the default, these countries have since reached donation rates as high as **90%** and above, while opt-in countries have failed to reach **15%**[22]
- Generic equivalents of brand-name prescriptions often work just as well as their counterparts, but are significantly cheaper. Physicians, however, often stick with brand-name medication which comes to mind more easily, and in doing so, fail to achieve easy savings for their patients. When researchers altered physicians' computer display to include an opt-out checkbox labeled "dispense as written", which prescribed the generic version, the overall rate of generic prescriptions rose 23 percentage points to **98%**, saving patients from unnecessary out-out-pocket expenses without compromising health outcomes[22]

[19]"Hassle Factors." *ideas42*, www.ideas42.org/blog/principle/hassle-factors-2/.
[20]Cherry, Kendra. "How the Status Quo Bias Influences the Decisions You Make." *Verywell Mind*, 14 June 2019, www.verywellmind.com/status-quo-bias-psychological-definition-4065385.
[21]Blau, "Deep Thought: A Cybersecurity Story.", 38.
[22]Shach, Ruth, and Lynn Zhao. "Using Behavioral Economics to Change Behavior: By the Power of Default." *Center for Advanced Hindsight*, 5 Oct. 2018, advanced-hindsight.com/blog/by-the-power-of-default/.

Nudge #8: Social Proof and Security Measures

Cognitive Bias | **Effect on Security Behavior** | **Suggested Nudge**

When people are unsure of an appropriate course of action, they look to those around them for guidance, a phenomenon dubbed **social proof**. People will do what others do, even if there is no reason to believe others are doing the smart, or right thing.

Security behavior has generally low observability. People don't know the strength of each other's passwords, or whether their friend has recently completed the prescribed software update. Thus, people **lack motivation** to make a concerted effort to improve their personal security behavior.

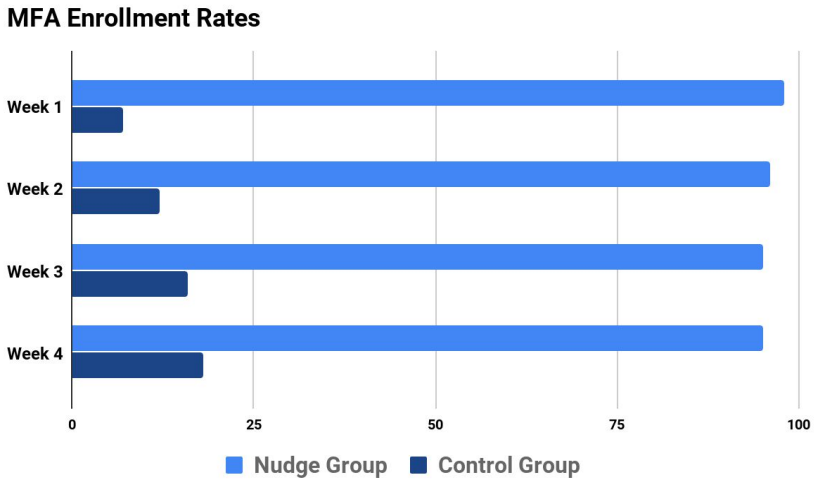
Simply **showing people the specific number of their coworkers that used security features**, without any subjective framing, can drive wide scale adoption of such features. Generally, as the proportion of users participating in safe security behavior increases, social proof messaging will see an increased ability to impact behavior.[23]

Evaluating the Impact of Nudges

As with any policy change, when it comes to the implementation of nudges, it is important to be able to measure impact, and the degree to which certain tweaks to the choice architecture are working as desired. The simplest way to get a clear picture of a nudge's performance is by randomly administering a given nudge to a sample of the office via a "**randomized control trial**", a research design frequently used in medicine. From there, the desired metric should be monitored, and compared between the sample that received the nudge, and the sample that did not. For instance, if an organization wishes to introduce MFA, and the accompanying default nudge, it should register half of its users in the opt-in design, and the other half in the opt-out design. In the case of this nudge, the metric of interest is the adoption rate of MFA, so that rate will be monitored and compared between the opt-in and opt-out groups over a period of time that the organization feels is appropriate. The difference in adoption rates between groups can be considered a quantitative measure of the nudge's impact.

*From the sample reporting templates below, it can be established that opt-in design resulted in a **79% increase** in MFA enrollment after 4 weeks. These data are not drawn from a real trial, but are meant as an example of reporting dashboards to be used in evaluation.*

Weeks Since MFA Introduced	Nudge Group MFA Adoption Rate (%)	Control Group Adoption Rate (%)
0	0	0
1	98	7
2	96	12
3	95	16
4	95	16



[23]Das, S., Kramer, A. D., Dabbish, L. A., & Hong, J. I. (2014). Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security* (pp. 739–749). ACM. doi:10.1145/2660267.2660271.

For organizations wishing to implement multiple nudges at once, measuring impact is notably more complicated. Simply administering all the nudges to one group, and comparing it to a control group will not provide accurate insight into the effect of individual nudges, since their effects can overlap in the way they affect security behavior. To detangle the effectiveness of nudges from one another, multiple test groups have to be formed, in which each test group is exposed to exactly one nudge. Metrics for each can be then be tracked and compared with those of the control group which received no nudges. However, the more test groups that are created, the more likely that evaluation will be somewhat biased, due to the way smaller groups compromise statistical robustness in experimental trials. Therefore, organizations of smaller size should take care when administering nudges, and be wary of conclusions drawn about the effects of a nudge from a sample of say, seven users.

Final Thoughts

Nudge theory attracted enough attention, from academia, businesses, and governments alike, that Richard Thaler, the scholar responsible for pioneering the idea, won the Nobel Prize for Economics in 2017. The concept of the nudge stirs up so much excitement, partly because of the essentially unlimited extent of opportunities in which the theory can be applied to drive positive change, ranging from the minor and inconsequential, to the sweeping and life-changing. Rarely is it the case that an Economics Nobel-Prize winning idea is both easily grasped and implementable by those that have not studied at a doctorate level, thus ignoring the potential of the nudge would be to leave valuable, actionable knowledge on the table.

As security and privacy breaches grow evermore threatening, organizations can no longer afford to ignore the role played by human behavior in exposing security systems to cripping financial and reputational risk. Nudges for cybersecurity present themselves as a promising tool, especially for organizations frustrated with the way their exhaustive security awareness efforts are in vain, and fall short of having the desired effect on their members' security behavior. The cost-effectiveness of the nudge makes implementation a low-risk investment, and its lack of forcibly controlling behavior makes it extremely palatable, and even inviting, from a user standpoint. Failure to incorporate nudges, or at least some element of behavioral science into an organizational security strategy will result in a persisting inability to realize the full potential of one's technical infrastructure, and is thereby equivalent to handicapping security posture.

ABOUT THE AUTHORS

Clare Suter is a Analyst Intern in DayBlink's Cybersecurity Center of Excellence and is based in the Vienna, Virginia office.

Jacob Armijo is a Senior Consultant at DayBlink and Chief of Staff of DayBlink's Cybersecurity Center of Excellence. He is based in the Vienna, Virginia office.

Justin Whitaker is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence and is based in the Vienna, Virginia office.

Michael Morgenstern is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence, a former cybersecurity entrepreneur, and is based in the Vienna, Virginia office.

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It is outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents. The way we do business is also changing – with more data stored and living in the cloud, and constant mobile demand. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cyber@dayblink.com
Call: 1 (866) 281-4403