Looking to behavioral economics, psychology, sociology, neuroscience, and other fields, we can understand cognitive biases and how we can better engage people to improve cybersecurity awareness, behavior, and culture. Scientists in these fields have studied human perceptions and behavior: How do we think, and why do we behave the way we do? We need to take lessons from these disciplines and apply them to how we can best communicate about, and raise awareness of, cybersecurity. The problem is that we can raise awareness around an issue without positively influencing behaviors. Awareness of cybersecurity is high now and has been for a couple of years. But that doesn’t mean that people are behaving the way we would like regarding matters such as password authentication and social engineering attacks.

We need to consider ways that we can better communicate about cybersecurity. For me, this involves understanding how people think. When we are communicating messages to people, how are they receiving our messages, and how are they reacting? A lot of this involves understanding what is known in psychology as heuristics, or “shortcuts in the brain,” which have a significant influence over how people behave. These are ways of thinking, ways of making a decision, that we are not necessarily aware of. But to get through our day of making decisions, we all rely on these ways of thinking, these shortcuts in the brain. When it comes to raising awareness about cybersecurity, I believe that five of these heuristics are particularly relevant: social proof; the optimism bias; the psychology of fear; the stereotype threat; and self-efficacy.

**Social Proof**

*When people don’t know how to act, they assume the behavior of others. Most of us are familiar with social proof, even if we might not know its name in the field of psychology. For example, TripAdvisor, Google reviews, Airbnb, and similar websites show what other people think about something. If you see that 90 people have given a service or product a four- or a five-star review, you’re more likely to give the service or product a try. That’s social proof, and it’s very powerful.*

Recent research has shown that when about 25 percent of a group start behaving in the same way, most of the other 75 percent of the people in that group will follow the behavior of the 25 percent.2 We think other people might know better.

The influence of social proof on behavior has been explored in many disciplines, including environmentalism and the attempt to tackle climate change. For example, some research has looked at hotels and the extent to which hotel guests will reuse their towels.3 Most people don’t reuse their towels; they want a new, fresh towel every day. This results in a large cost for the environment overall. Researchers investigated whether they could influence, by using social proof, the extent to which people reuse towels. In hotel bathrooms they put signs that said: “Most people in this hotel reuse their towel to help save the environment. Will you please do the same?” The researchers found that people who saw these signs were more likely to reuse their towel. Next, to see if they could make the social proof even more persuasive, researchers tried another sign that said: “The last person who stayed in this hotel room reused their towel. Will you do the same to help save the environment?”

The use of social proof has not been explored in the area of cybersecurity. Instead, we may be inadvertently using social proof against ourselves. Most of the messaging...
We need to consider ways that we can better communicate about cybersecurity. This involves understanding how people think.
around cybersecurity and behavior is very negative. When we tell people, “Here’s a list of really bad passwords that most people are using,” individuals think, “Everyone else has a bad password, so it can’t be that important for me to have a good one.”

How can we get social proof on the side of cybersecurity communications and awareness raising? One simple example is phishing simulation exercises. When an exercise is over, what message do you put out? Do you say that 30 percent clicked on the link (bad!), or do you say that 70 percent did not click on the link (good!). It is more effective to promote the number of people who did not click the link than the number who did. Next time, join your colleagues in being part of the majority. If we want to encourage people to practice more secure behaviors online, we need to start highlighting the positive behaviors of others.

The Optimism Bias
People underestimate the likelihood of bad things happening in their future and overestimate the likelihood of good things happening. Most people are optimistic. Research conducted by a team of neuroscientists over the last ten years found that about 80 percent of people are wired toward being optimistic. No matter what messages or what facts we give people, they remain optimistic.

For example, researchers conducted a study in which people were asked how likely they thought it was that they would get a disease such as cancer. When individuals replied that they thought they had a 10 percent chance of getting cancer throughout their lifetime, the researchers told them the facts: they had about a 30 percent chance of developing cancer. Nevertheless, the study participants were reluctant to let go of their optimism: the average response then was, “OK, maybe I have an 11 percent chance.”

In the area of cybersecurity, no matter what facts we give people and no matter how much we tell them where hacks have happened, how likely they are to be hacked, and the harmful influence a hack will have, people are going to retain their optimism. When cybersecurity professionals are faced with a nontechnical person who displays this kind of stubborn optimism, they usually respond with more facts. Someone might say: “Why would hackers want my data? That’s not something I need to worry about.” Cybersecurity professionals often respond by providing more statistics: how many cyberattacks occur, how much money they cost people, the negative impacts that can come from a cyberattack or data breach, and the extent to which the problem is increasing. Yet these statistics very rarely change people’s minds.

The good news here is that optimism makes people try harder. While using a tone that is more optimistic and more empowering, cybersecurity professionals can tell people: “The threat is real, but you can do a lot of things that are quite straightforward and that will bring the threat down to a great degree.” Even though optimism is generally more powerful than facts, when people feel that there is a point to changing their behavior, that they can actually make a difference in their level of cybersecurity, they are more likely to engage in the behaviors we recommend.

The Psychology of Fear
Fear has to be handled very carefully in order to motivate positive behavior change. The traditional cybersecurity approach has been deeply rooted in fear, uncertainty, and doubt. The bad news about this traditional approach—telling people something scary because we think it will lead to better behaviors—is that it simply doesn’t work. Research has been conducted analyzing six decades of what is known as fear appeals: using fear to try to change behavior. What these sixty years of the use of fear appeals have shown is that to use a scary message effectively, you
need to communicate that message very carefully. When people are confronted with something scary, such as a threat, they naturally appraise that threat and consider how real it is.

People need to understand that a threat is serious and that it applies to them before they will even consider some of the recommended behaviors to avoid it. Only then will they consider the behaviors and whether they are capable of enacting the recommendations. For example, when we’re told to use different and complicated passwords for each account, when we’re asked to turn on two-factor authentication, when we’re instructed not to click on suspicious-looking links, we think: How am I going to do that? And only if we feel able to do that will we engage with the actual danger. If we feel that those responses are beyond our reach, or that they wouldn’t make a difference, we ignore the threat.

Fear appeals can therefore be a very damaging way to spread the message about cybersecurity. A much more empowering way to communicate about cybersecurity is to highlight the positives that come from good cybersecurity. An example from the public health arena can help us understand why this is a better approach. A set of hospitals in New York State set out to address the issue of doctors and nurses who were not sanitizing their hands while they were on shift. The hospitals put in a system of surveillance to encourage doctors and nurses to use hand sanitizer and to wash their hands more regularly. The researchers found that when they told the doctors and nurses about the surveillance, compliance with hand sanitation rose 10 percent. They then installed, above every hand-sanitizer stand, an electronic sign that popped up with a smiley face and a message that said “good job” when doctors and nurses used the stand. Next the researchers added an electronic sign in the common area, tracked hand-sanitizing by shift, and introduced an element of gain: the shift with the highest amount of hand-sanitizing was rewarded. When they took this more positive approach, compliance increased by over 90 percent. These results were replicated in other hospitals.

People are drawn more to a positive message than to a negative message, motivated more by good feedback than by fear.

The Stereotype Threat
The burden of a stereotype makes people unintentionally confirm it. If individuals or groups enter a situation in which they know they are the subject of a stereotype, knowledge of that stereotype will be such a burden and
When it comes to cybersecurity, a stereotype that ferociously dominates this industry is that people are the weakest link, that humans are the problem.

As stated by Emma W, People-Centred Security Lead from the UK National Cyber Security Centre: “If security doesn’t work for people, it doesn’t work.” Instead of undermining people, let’s start spreading a more empowering message.

**Self-Efficacy**
A person’s increased belief in their ability to succeed in specific situations or to accomplish a task—that is, their self-efficacy—drives better behaviors. We know this from research that has been done not only around levels of empowerment and self-efficacy but also around levels of confidence in information security.6 This research has found that people who feel more confident about cybersecurity are more likely to pursue the behaviors we recommend, such as doing their updates, having a strong approach to passwords, using good cyber-hygiene. This comes from having a feeling of confidence and a feeling of being able. If we give people the encouragement and the tools they need, they will practice more secure behaviors. For example, implementing a “report a phish” button in your emails gives people a quick and easy way to report suspected phishing emails. They have a mechanism, a tool, with which they can engage in good cybersecurity.

This positive effect of self-efficacy is supported by the psychological research on how people respond to fear appeals.2 When we are discussing cybersecurity, we are inevitably talking about things that are scary: threats, crimes, and malicious behavior. People can often feel intimidated by the subject, and they cannot escape from the need to talk about something that evokes fear. This is why efficacy messages are so important. If cybersecurity professionals talk about something scary without providing a strong efficacy message, listeners will engage in controlling the emotional response to fear rather than in controlling the danger itself: “If fear appeals are disseminated without efficacy messages, or with a one-line recommendation, they run the risk of backfiring, since they may produce defensive responses in people with low-efficacy perceptions.”3

Psychology research has shown the importance of empowering people and raising their sense of self-efficacy in order to positively change their behaviors. If we do not focus on efficacy by carefully communicating what people can do to better protect themselves online (e.g., use strong, unique passwords) and how they can do so (e.g., use a password manager), then we may find that our awareness-raising efforts will have a negative impact.

**Conclusion**
These five shortcuts in the brain, or ways of thinking, all relate to how we frame our messages. With a deeper understanding of psychology, behavioral economics, neuroscience and sociology, we can make our messages much more engaging and much more impactful. By...
getting social proof on our side, harnessing optimism, spreading hope instead of fear, resisting stereotypes, and raising self-efficacy, we can be more effective in our cybersecurity awareness-raising, leading to more positive behavioral change and stronger cybersecurity cultures.

Notes

© 2019 Jessica Barker. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Jessica Barker (jb@cygenta.co.uk) is Co-Founder and co-CEO of the cybersecurity consultancy Cygenta (www.cygenta.co.uk), where she follows her passion of positively influencing cybersecurity awareness, behaviors, and culture in organizations around the world. She has been named one of the top 20 most influential women in cybersecurity in the United Kingdom and in 2017 received one of the UK’s TechWomen50 awards.