Cognitive Bias & Cybersecurity - Mosquito versus Shark

Cybersecurity is a people problem, driven by our perception of risk. Tools help. In fact, tools are incredibly necessary but tools are also only as good as the people implementing them. Also, the work culture has a huge impact on behavior because employees tend to gravity toward the middle of the group, modeling their behavior to fit in, and be accepted as part of the team – for better or worse from a security best practices standpoint.

67% of security breaches are due to human behavior, not the failure of tools.

People have to digest a lot of information and success often means navigating that information efficiently, making decisions quickly – like to avoid getting in an accident on the freeway. But, that quick decision-making is not helpful during a cyberattack. People have unconscious biases that often serve them well in the workplace in general but can be catastrophic when exploited by a hacker.

Cognitive bias – There are so many categories of cognitive bias, each defined and labeled differently by the experts. Rather than try to examine and exhaust each, i.e. more information overload, here are 10 types of cognitive bias:

1) Anchoring – I looked at some of the information and my mind is made up.
2) Confirmation bias – The opposite of anchoring – I know what I will find, if I look. Oh, there, I looked and yep, I found what I was expecting to find.
3) Herd behavior – That person is not concerned about changing their password and they have never been hacked, so why should I go to the trouble?
4) Choice/Decision fatigue – There are so many cybersecurity tools available, which one is best? Do I need another? Plus, a constant barrage of work, meetings, information, alerts, tools and I don't know where to start. So, I will play wordle instead.
5) Optimism bias – I put security protocols in place and I hired good people, my job is done.
6) User Fatigue – I have followed all the rules and now you want me to update my whatever again, I am tired of updating and I work too much to have to worry about this again.
7) Alert Fatigue - Too many false positives lead even the most conscientious employees to start ignoring all alerts.
8) Ostrich approach – Head down on my work, not on security. La la la… What security issue, I cannot hear you!

9) Placebo effect – I put security practices in place when I started the company. I am covered.
10) Parkinson's Law of Triviality (Bikeshedding) – Employees often deal with a lot of trivial tasks and not enough time on the big impact items as it relates to overall corporate security. Sometimes this is due to the complexity of security issues. People gravitate toward doing what they know versus spending the time to learn the more difficult parts.

You can observe cognitive bias play out in real-time on Facebook. Either a person has friends who agree with them 100% of the time or the dissenter is mocked and blocked. That person's page becomes an echo chamber where they only hear opinions that precisely match their own. Therefore, they must be correct. Others allow a "troll" to attack and berate a topic they care very much about and the user becomes depressed and despondent that the entire world has gone mad, is uncaring, and resolving this issue is beyond hope. All is lost.

Information is not only as good as the source; it is as good as the user. Are you afraid of a shark or a mosquitos. I say shark! But, mosquitos kill more people each day than sharks kill in 100 years. Interesting point… Of course, head to head, I think I might be able to take the mosquito, not the shark.

Education, training, and explaining cognitive bias to everyone in the organization makes all those investments in cybersecurity tools much more valuable.