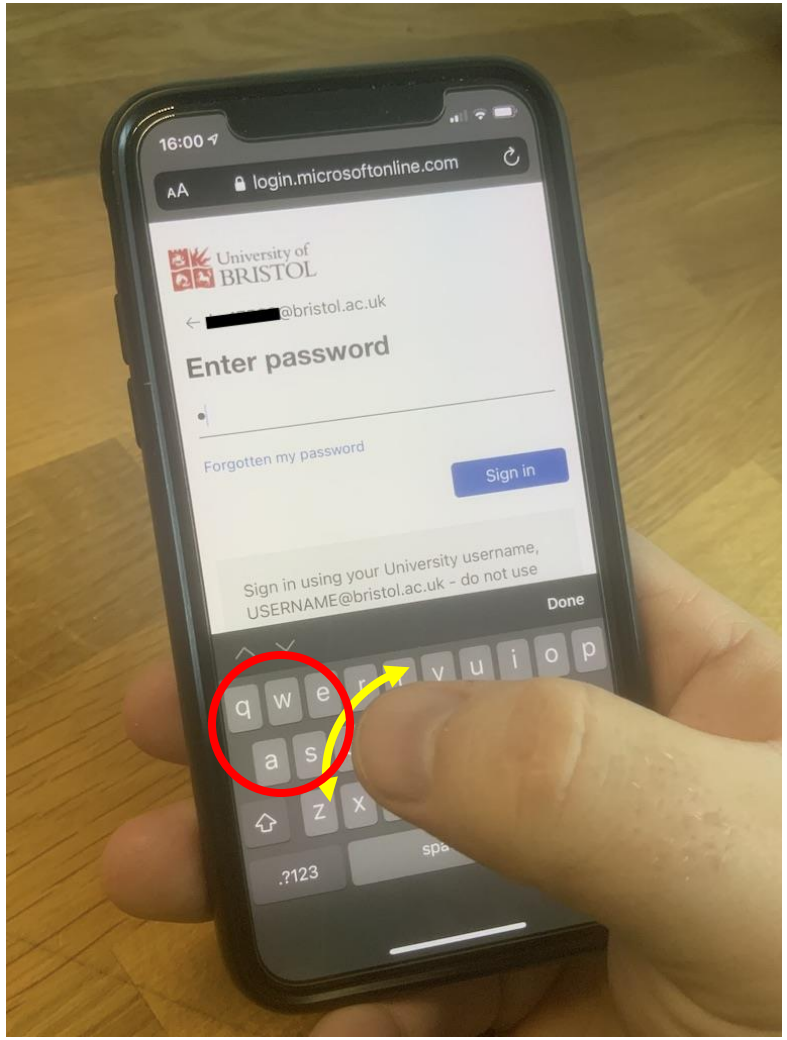
# the role of bias (part b)

# So to physical bias (aka constraint)




We seem to be looking back at prior lectures a lot, and here is no exception. Usable Security again and physical contexts.

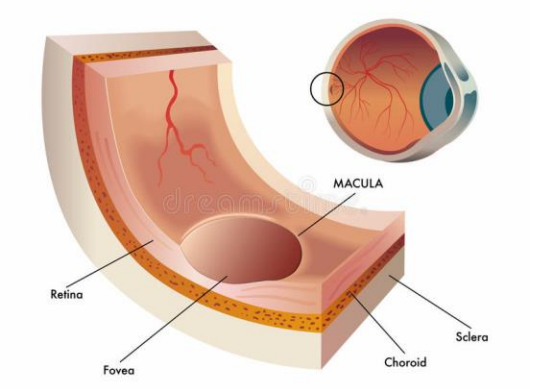
My friend owns an iPhone X. Like many people he uses a phone single handed.

BUT he has fairly short fingers and his thumb cannot cover the width of the screen.

**So might this mean that there are five fewer characters in his passwords based on physicality?**

And there are lots of physical limitations that we, as animals have. Some of them matter with security.

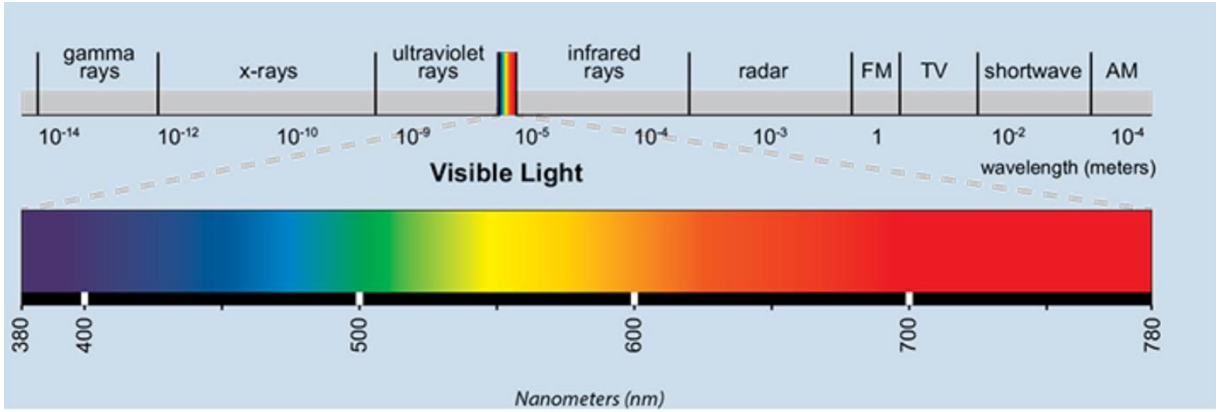
# Vision

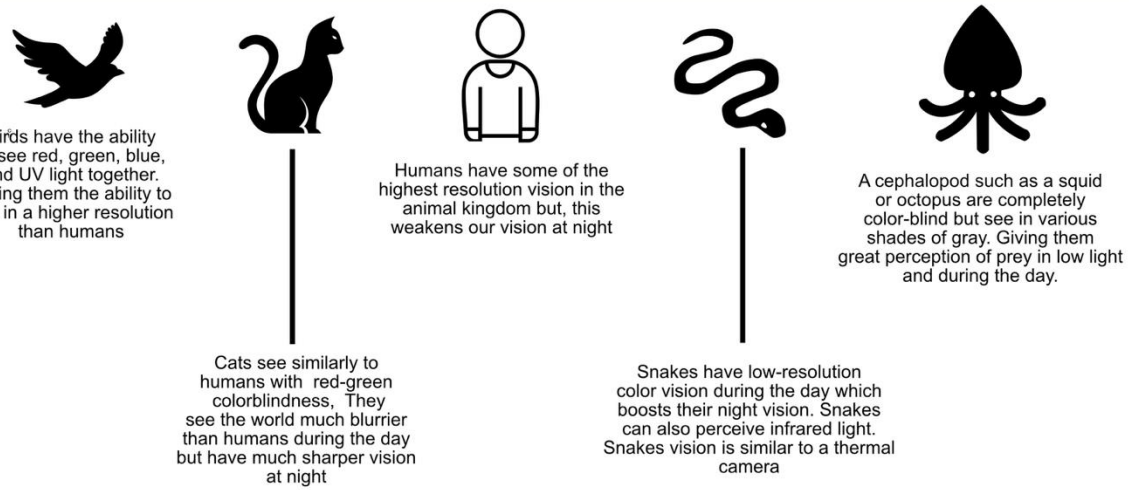


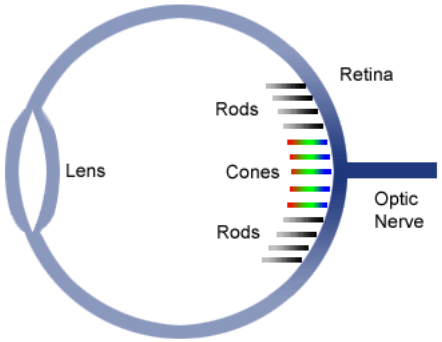

Humans are animals, primates specifically. And we are hunters. Our eyes are on the front of our faces, providing binocular vision good for tracking prey.

Prey animals, on the other hand, have their eyes to the sides (or top with some fish). This provides them better angular coverage, to spot the hunter incoming.

And it doesn't stop there. Our eyes are different as well. In humans the fovea (the bits that provide the super clear vision) are limited to that front facing cone, with peripheral vision being demoted in functionality [more on next slide]




We all are aware that humans have a range of the light spectrum we can see (from deep blue to deep red). Hopefully everyone is also aware different animals see different parts of that spectrum.

But, as mentioned a minute ago, the specialisation of front facing highly focussed vision comes at a cost.

Firstly, our colour vision is limited to the most central of cones. Those used in full focus. The rest, the peripheral is reduced to to fuzzy greyscale (trust me it's not in colour). We compensate for this with very fast scan times (c.20ms) and the ability to stitch together multiple images to give a view on the world.

Secondly, that picture is vast in complexity – too vast for our brains to comprehend - so to cope with our limited capacity we discard a lot of information.

Remember the gorilla?

Combine these visionary constraints with a cognitive bias and wonder what else of the world do we miss?

# Fakery – Further Compounding Constraints

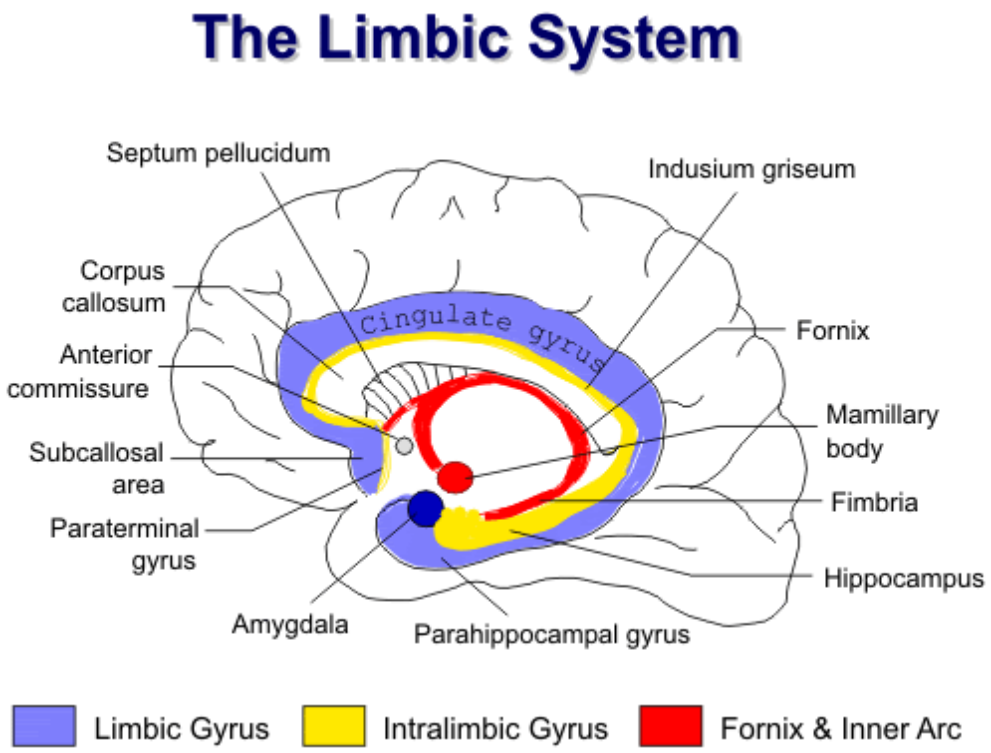
Other people are fully aware of those physiological quirks AND often the cognitive ones that when aligned make error more likely.

Take sports. In most team-based ball sports the dummy or fake is taught. It's designed to fool the opponent into thinking you are doing one thing whilst actually doing another. That visual refresh rate (c.20ms) readily comes into play.

But there are less benign uses of fakery. Take the example of Three Care Monte. It is a sleight of hand street hustle. A malevolent version of illusion. Using distraction, focused attention & both auditory and visual cues people are suckered out of money thinking the game is simple. It isn't. It's rigged.

Attention is selective (search for Posner's spotlight model of attention). Why? Because attending to all stimuli sufficiently is computationally infeasible. It would place great demand on (among others) the working memory system, i.e., a cognitive capacity issue.


# A final physiological constraint – the limbic system.




The human brain is an incredible 1.5kg lump of stuff. And whilst our cognitive capacity is all held up there, there are even physiological issues we have to handle. In this case the limbic system (the blue bit).

It is responsible for regulating emotional responses (amongst other behaviours) for example, the freeze, flight/fight mechanism when presented with a perceived threat.

So why is this important for cyber security?

These emotional responses can be, and are, exploited by malicious actors because the limbic system can overpower the logical parts of our brain.

Think how the pretexts of phishing emails target emotional responses, using urgency or authority to panic potential victims into clicking on links they normally would avoid.

# It’s not all bad, there is something simple we can do to help

So despite, as humans, all being replete with both cognitive and physiological bias - there are things in our toy boxes that can help navigate these waters.

In fact you are doing the very first.  Being aware of these things even existing.  You can go further.  You can improve your meta-cognitive abilities to be better aware of how you think and make decisions.

e.g., if you get an email from your *insert country here* long lost relative offering up millions in lost inheritance into YOUR bank account, but needing an immediate response….

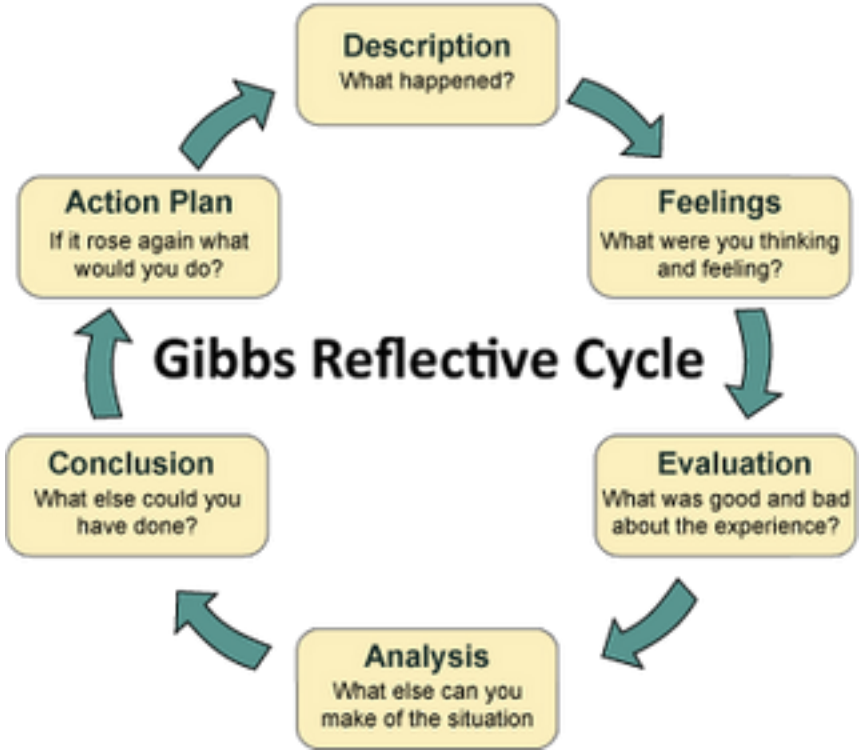
Recognise how that makes you feel!  Is there a rush of excitement, or a gut feeling?  Use that feeling to switch to your system 2 (slow) thinking and take rational objective information based decisions.

# Reflective practice

To help you with that meta-cognition, a form of reflective practice (e.g., Gibbs 1968) can help you look back (and reflect) on how you have handled situations before so that you can, through continuous learning, identify and work on your own personal biases.

I know this might sound a little… icky. But it's a normal practice, especially in sport science. Understanding past performance is critical to improvement.

It's tightly aligned to the Just Culture aspect of error in enabling reflection on when and why things went wrong so we can iteratively design them out.



# But don’t over-correct

People who have fallen foul of scams, for example, are known to reflect in an almost self-destructive manner. In doing so they over-correct their actions in an attempt to avoid the same outcomes.

So perhaps someone fell for a phone support scam, and as a result installed multiple pieces of security software thinking they would make them **more** secure.

In reality this is essentially a Dunning-Kruger.  Those bits of software may well interact in unknown and insecure ways (as they were likely never designed to work in cooperation).

# Mull on these for the AMA

Are you aware of any cognitive biases you may have?  What are they?

How might they impact your ability to be secure (either personally or in your work)?

How might Usable Security help / hinder bias?

Can you think of any other cognitive biases from the codex which might have likely implications for cyber security, and how?

# next time
# security ergonomics by design