error in practice (part b)

As Engineers,
As Designers,
As Practioners…

Cater for very real human constraints, and **make things usable**

AS WELL AS

Avoiding that shift in error to ourselves, and overcome our own fallibility and, in turn, **avoid baking in failures** to the things we build

How can we cater for failure?

Better design using frameworks such as Privacy, Security and Security Ergonomics by Design.

However, to design systems to cater for human error in a graceful and resilient way you first have to understand

How people and systems have failed before otherwise we get headlines like…

Useful Stuff

Cavoukian, A. 2009. Privacy by design: The 7 foundational principles. http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

NCSC. Secure by Design. https://www.ncsc.gov.uk/collection/cyber-security-design-principles

Craggs, B & Rashid, A. 2017. Smart cyber-physical systems: beyond usable security to security ergonomics by design. https://doi.org/10.1109/SEsCPS.2017.5

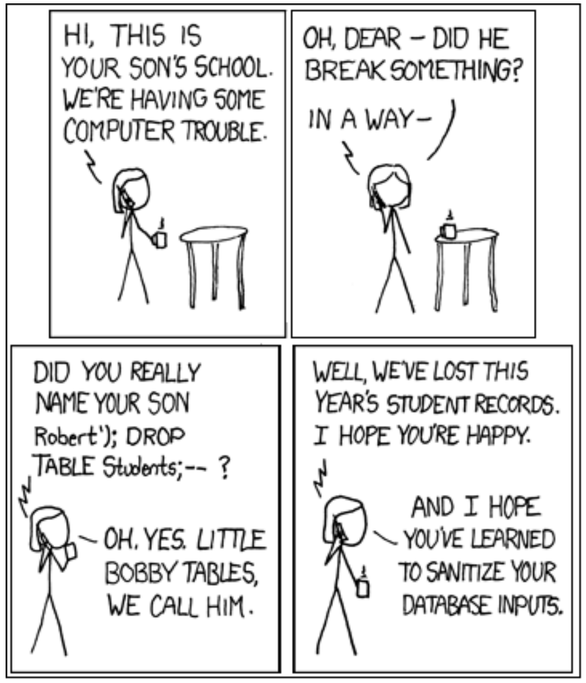
But “Sophisticated” ???

```c
#include <stdio.h>

int main()
{
    char a_chBuffer[100];

    printf("What is your name?\n");
    gets(a_chBuffer);
    printf("Hello, ");
    printf(a_chBuffer);
    printf("!\n");

    return 0;
}
```



We’ve known about buffer overflow attacks since the Morris Worm (1988) and format string errors (1989). SQL injection attacks since 1998.

Yet in 2020 Akamai estimated variants of SQL Injection accounted for 65% of attack vectors 2017-19! WhatsApp had a buffer overflow CVE logged in 2019.

Latent failure that is over 20 years old isn’t sophisticated. We need to capture and learn from these failures to stop re-implementing them.

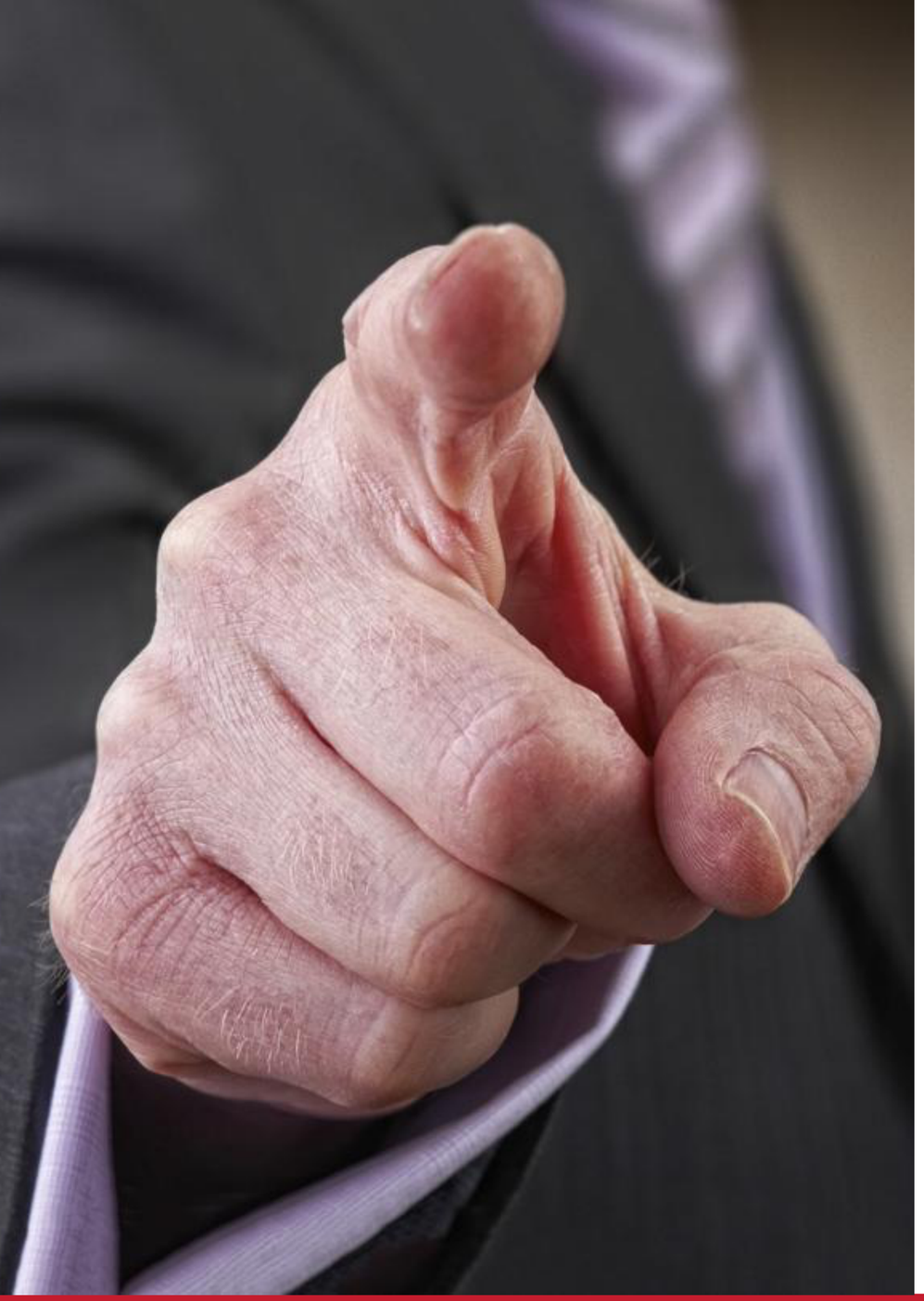
Useful Stuff

OWASP
SQL Injection Attacks
https://owasp.org/www-community/attacks/SQL_Injection

Wikipedia !!!! Buffer Overflows
https://en.wikipedia.org/wiki/Buffer_overflow

Wikipedia!!! Format Strings
https://en.wikipedia.org/wiki/Format_string_attack

NIST. 2019. WhatsApp Buffer Overflow CVE.
https://nvd.nist.gov/vuln/detail/CVE-2019-3568



Blame Cultures are NOT Helpful

As humans we are often quick to apply blame to overcome the discomfort of not knowing the cause of error or failure.

But when blame is applied to error, parties are keen to separate themselves from being held accountable.

And when the users, owners, developers and maintainers of a system all actively seek to avoid what might be a punitive situation, the facts of what and how something occurred become lost in obsfucation.

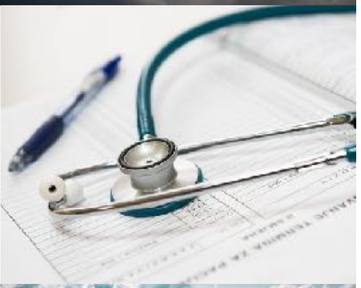



And Error Can Be Useful

As young children we failed A LOT. From those early attempts to stand and walk, to crashing our bikes, to learning to play an instrument. We erred all the time. It's natural. It's fundamentally important with learning.

We fail, we learn, we improve. It's how evolution works.

What really matters is that we don't keep repeating the same mistakes time and time again. In security those repeated mistakes are the vulnerable points at which attacks are targeted.


Capturing and Designing Out Latent Failure

The safety aware industries - and by now it should be no surprise - have long understood that not only must we design systems that cater better for human (active failure) error, but that the normally fatal consequences of not learning from accidents means they will simply reoccur.

And more recently even software development companies like Etsy have evolved to recognise that developer error is detrimental to operations.

Useful Stuff

Allspaw, J. 2012
Blameless PostMortems and a Just Culture.
https://codeascraft.com/2012/05/22/blameless-postmortems/

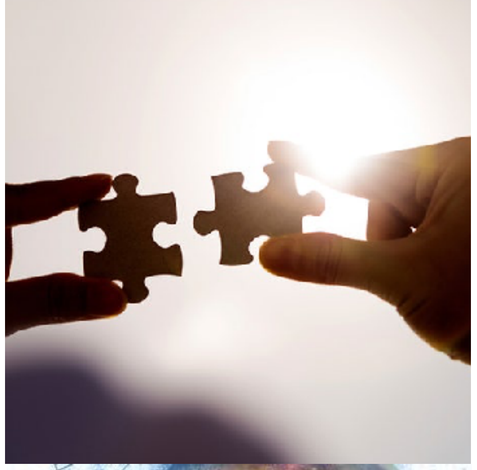
Just Culture

"a culture of trust, learning and accountability" Dekker 2018

A safe environment within which security incidents are captured, evaluated and *post-mortemed*, without automatic blame, in order to provide detail into the Security Ergonomics approach for the design of safe and secure cyber-physical systems.

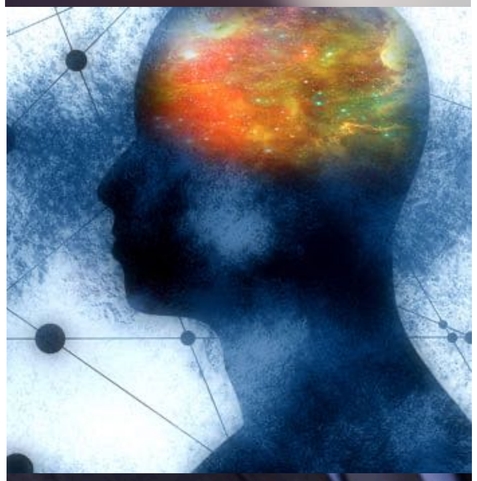
[note: we look at Security Ergonomics by Design in lecture 10]

The Benefits of Being Just



Insight

Clear picture of what is going on in organisation. Almost impossible to gain a “complete” understanding, from multiple viewpoints as to what actually occurred without a Just Culture.

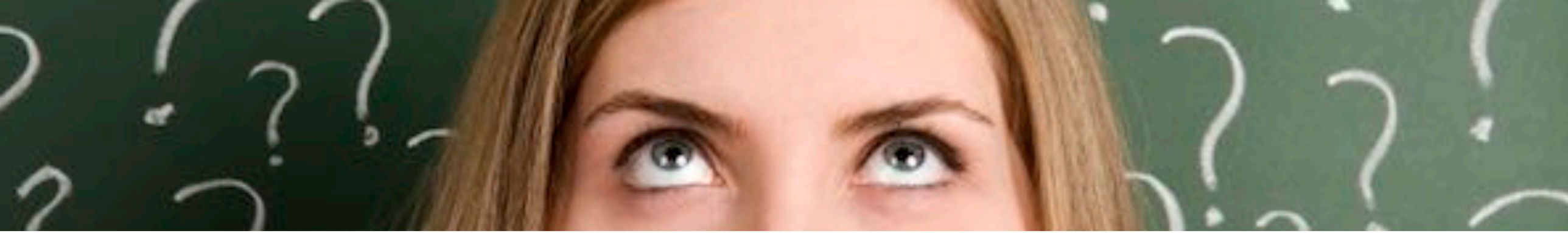


Wellbeing

Practitioners will suffer less anxiety… in the wake of an incident. Without a Just Culture it can be detrimental to commitment, job satisfaction and a willingness to step outside defined role.

Innovation

Focus can remain on long-term strategic investment in safe & secure products rather than priorities ending up focussed upon minimising short-term liability.



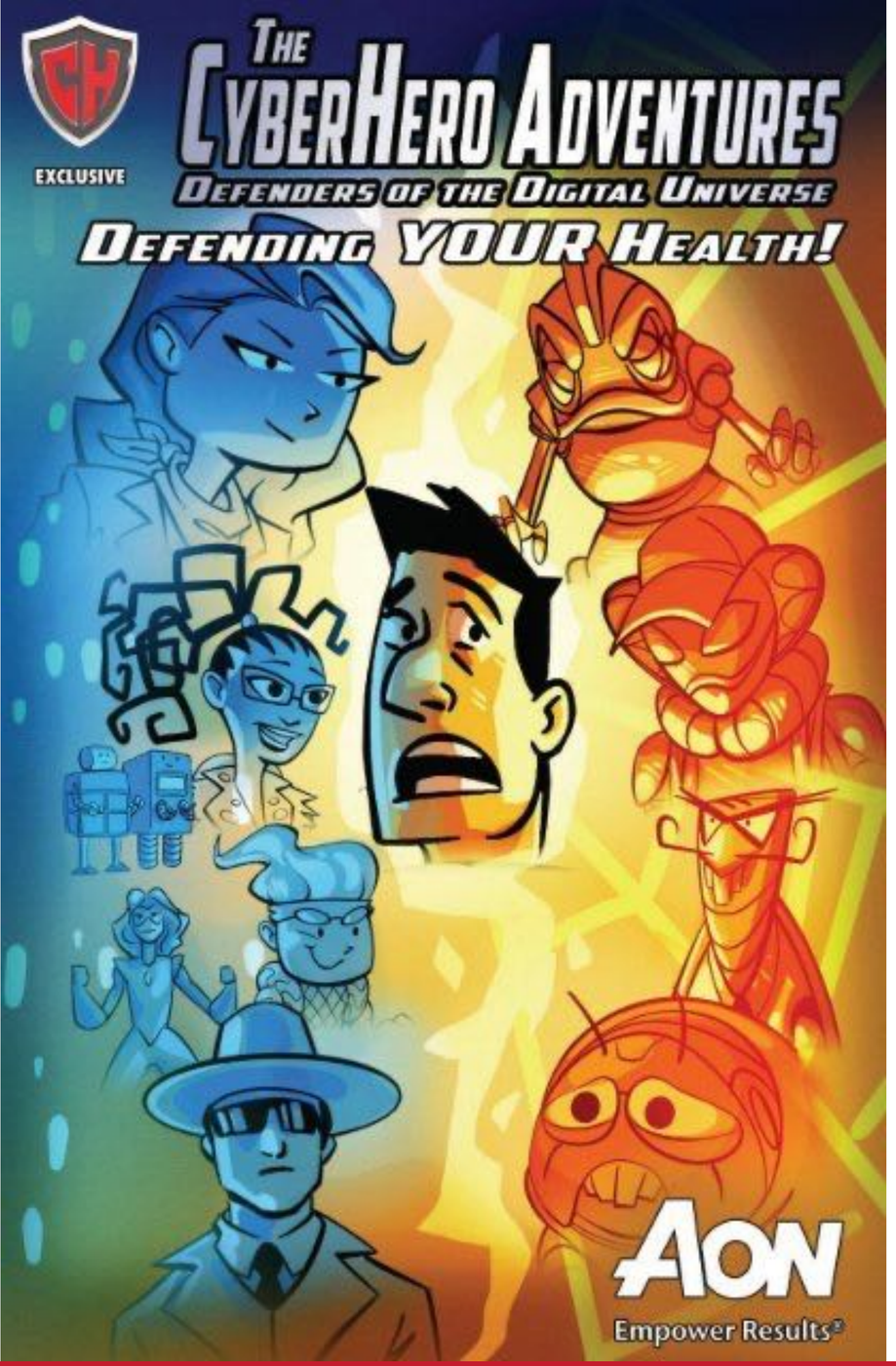
Considerations

To achieve a culture of trust, one in which people will report errors, accidents and near-misses, the processes by which the report is made, handled, discussed and acted upon needs to be defined and clearly signposted for people to use.

1. **Who gets to draw the line between acceptable & unacceptable behaviour?** Some lines can be set by consensus or committee, whereas others may be determined based on regulation or individual opinion.

2. **What role does expertise have in setting this line?** Is there a need for domain expertise to determine what is aberrant behaviour?

3. **How well insulated are internal processes and data?** Can external parties / agencies lift veil of privacy to potentially attribute blame to an individual?



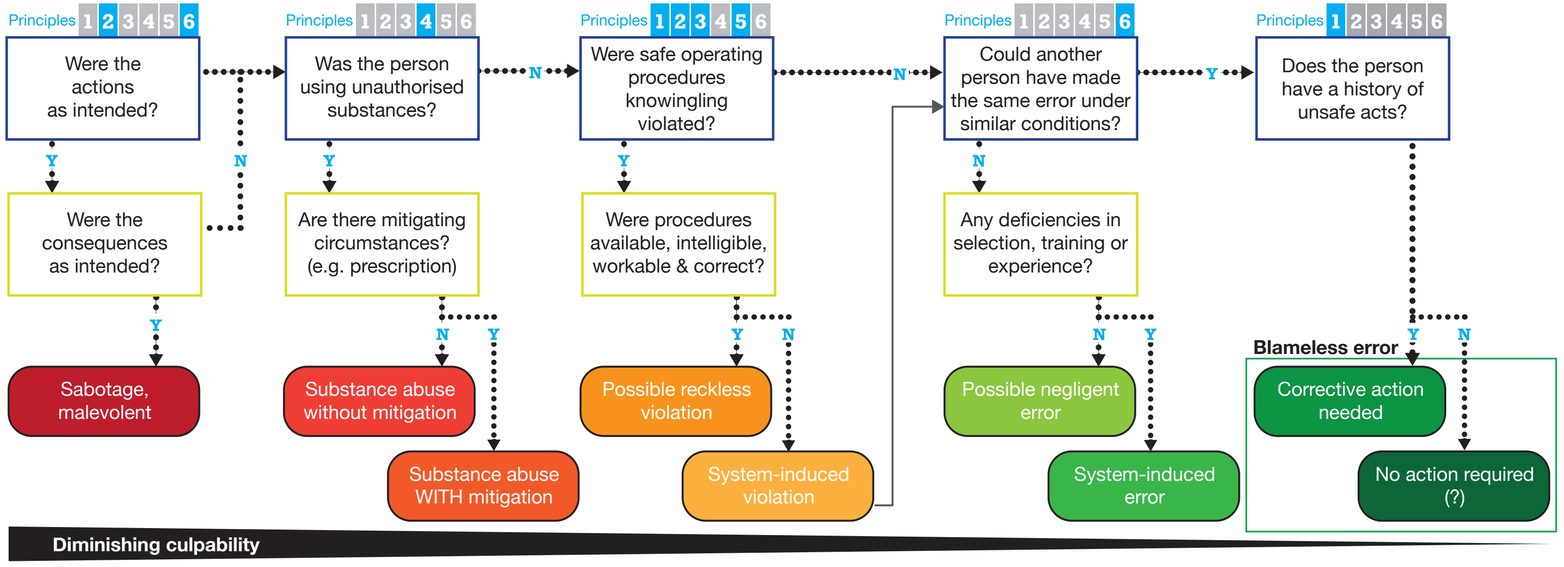
Aren't We All Possible Heroes?

Just like Sully, the captain of the plane that only landed safely on the Hudson because of extensive expert training. Just like Marcus Hutchens who stumbled upon a cyber attack flaw that saved time, money & probably lives I would argue that everyone who learns from their mistakes, reports them, documents the events and makes tiny system improvements to design out latent failure is a hero.

Culpability

Unlike blame-culture, culpability looks to the extent of the individual's responsibility for aberrant events.

Using defined method such as a decision tree; blame is reserved for deliberate subversive behaviour, with diminishing responsibility the more that behaviour becomes either inevitable due to system design.

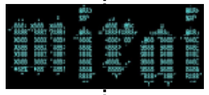


A Task…

Deliberate

Active Failure
(Human Error)

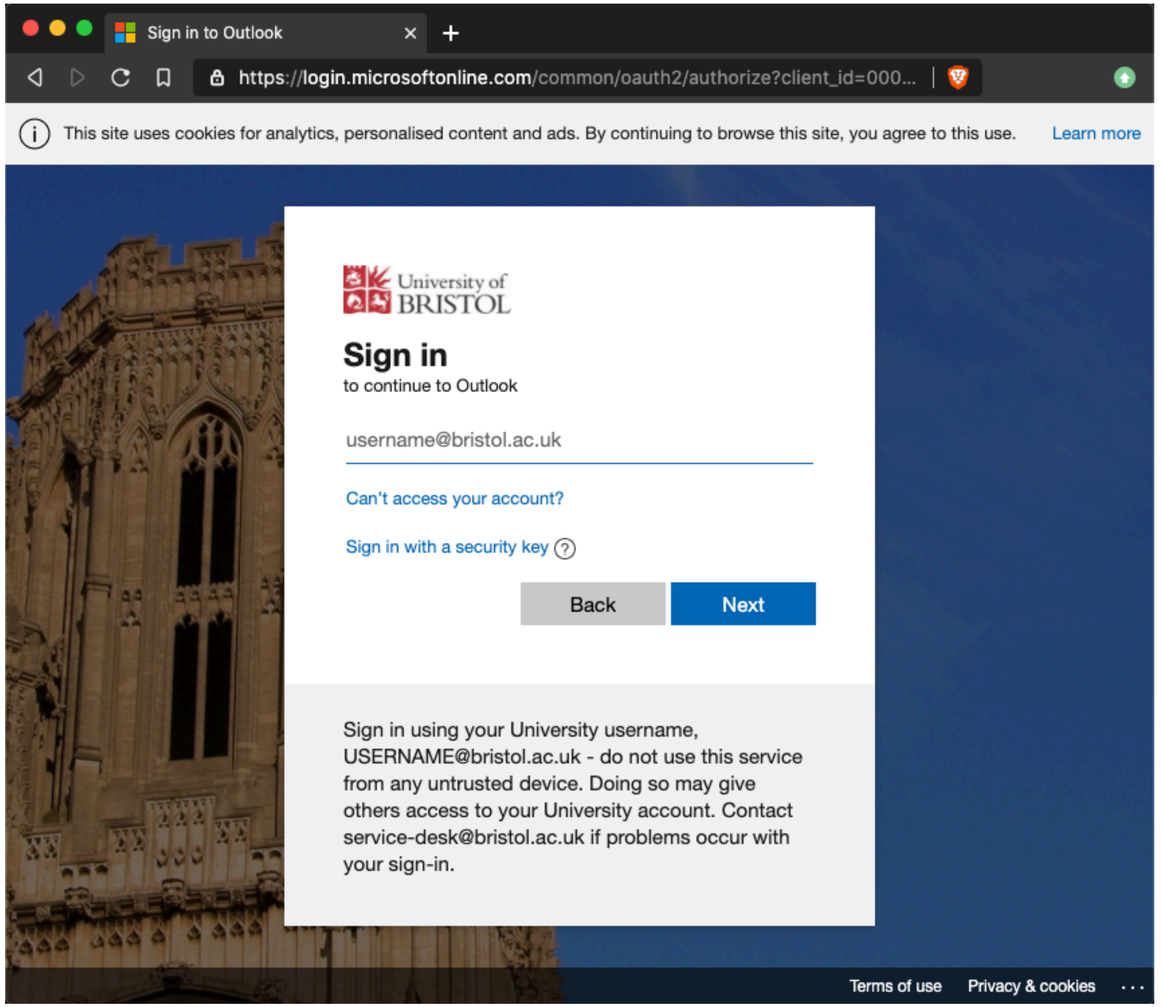
Latent Failure
(Design Flaw)



Inadvertent

Something to mull on for next time…

What is wrong with this UoB single-sign-on dialogue?



next time…
the role of biases