SECURITY (COMP0141): SECURITY BEHAVIOUR

HOW TO IMPROVE

Users lack intuition about complex computing devices →
Provide security education and training

Users are in charge of their own (complex) devices →
Make security invisible

It is hard to estimate risks →
Help users build more accurate mental models

Security measures feel like they get in the way →
Make security the path of least resistance

AWARENESS, EDUCATION, AND TRAINING

Awareness: why security matters and how behaviour affects it

- Make people realise security applies to them
- Principles from advertising: brief, unexpected, funny, visual

AWARENESS, EDUCATION, AND TRAINING

Awareness: why security matters and how behaviour affects it

- Make people realise security applies to them
- Principles from advertising: brief, unexpected, funny, visual

Education: increase knowledge of threats and impact

- Change perceptions of and attitudes towards security
- Need to be positive (not just “don’t”), realistic, and persuasive

AWARENESS, EDUCATION, AND TRAINING

Awareness: why security matters and how behaviour affects it

- Make people realise security applies to them
- Principles from advertising: brief, unexpected, funny, visual

Education: increase knowledge of threats and impact

- Change perceptions of and attitudes towards security
- Need to be positive (not just “don’t”), realistic, and persuasive

Training: build competencies and skills

- Replace bad habits with good ones
- Cannot be achieved via annual computer training!
- Need monitoring and corrective feedback

HOW TO IMPROVE

Users lack intuition about complex computing devices →

Provide security education and training

Users are in charge of their own (complex) devices →

Make security invisible

It is hard to estimate risks →

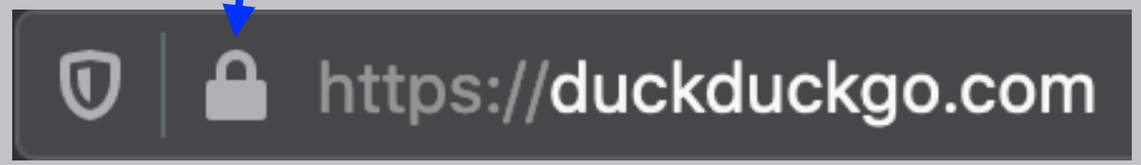
Help users build more accurate mental models

Security measures feel like they get in the way →

Make security the path of least resistance

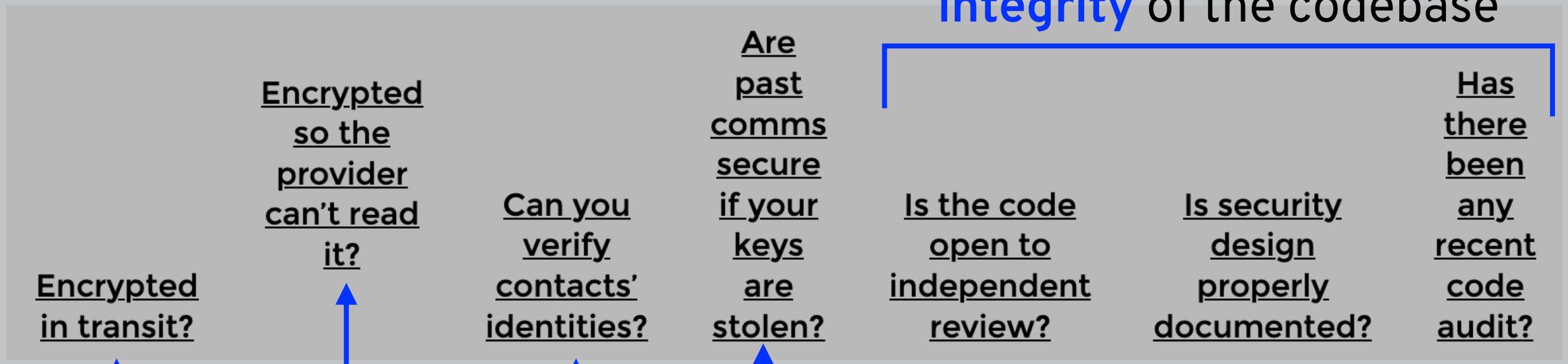
SECURE COMMUNICATION

no real sign of it, but your traffic
is encrypted (and thus secure)



SECURE MESSAGING SCORECARD

The EFF secure messaging scorecard evaluated messaging apps using a variety of different criteria



confidentiality against an eavesdropper

confidentiality against a curious service (E2E encryption)

integrity against impersonation (next week)

confidentiality (Week 10)

SECURE MESSAGING SCORECARD

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?
FACEBOOK	yes	no		
IMESSAGE	yes	yes		
SIGNAL	yes	yes		
TELEGRAM	yes	no		
WHATSAPP	yes	yes		

MISCONCEPTIONS

Futility: Service providers / intelligence agencies / attackers are all-powerful so there's no point in trying to be secure

Usability: Apps with a good usable design are more secure

Lack of prudent paranoia: Why would anyone want to read my messages anyway?

Security by obscurity: Open source schemes are less secure than proprietary ones

Fail-safe default: Assume security is always there (but apps like Telegram have two modes)

HOW TO IMPROVE

Users lack intuition about complex computing devices →

Provide security education and training

Users are in charge of their own (complex) devices →

Make security invisible

It is hard to estimate risks →

Help users build more accurate mental models

Security measures feel like they get in the way →

Make security the path of least resistance

WHY JOHNNY CAN'T ENCRYPT


Why Johnny Can't Encrypt

A Usability Evaluation of PGP 5.0

ALMA WHITTEN AND J. D. TYGAR

Only 2 out of 12 participants were able to complete tasks of:

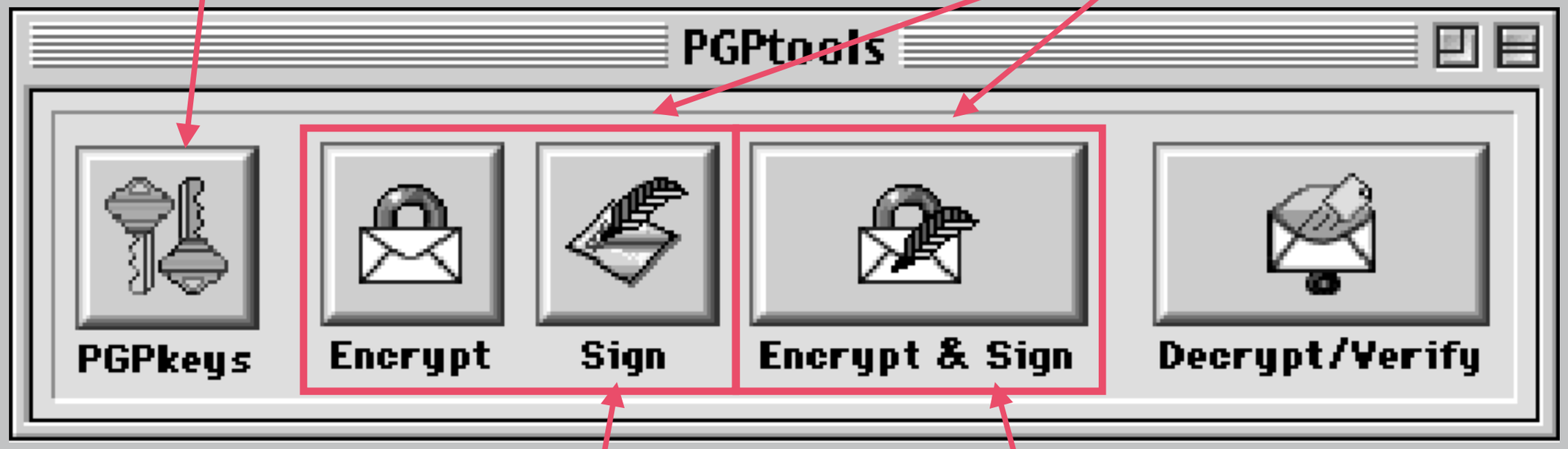
- Generating keys
- Sending encrypted messages
- Decrypting received messages

Some thought they were sending encrypted messages but were actually sending the plaintext - lack of usability led to issues with both availability and confidentiality

WHY JOHNNY CAN'T ENCRYPT

keys in real life are *symmetric*, but here they're *asymmetric*: you can't decrypt things you encrypt (**wrong mental model**)

what's the difference?



signing is misleading - what does it have to do with encryption? (**wrong mental model**)

lack of feedback once you click (what did I just do?)

SLIPS VS. MISTAKES

Slips (right intent, wrong action):

- Caused by inattention
- Fixed with better design, fail-safe defaults
- Likely to occur when users deviate from a routine

Mistakes (wrong intent)

- Caused by a mismatch with the user's mental model
- Error in planning
- Fixed with better knowledge and feedback

WHY JOHNNY (STILL) CAN'T ENCRYPT

Why Johnny Can't Encrypt

A Usability Evaluation of PGP 5.0

ALMA WHITTEN AND J. D. TYGAR

Why Johnny Still, Still Can't Encrypt:
Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University

Why (Special Agent) Johnny (Still) Can't Encrypt:
A Security Analysis of the APCO Project 25 Two-Way Radio System

Sandy Clark Travis Goodspeed Perry Metzger Zachary Wasserman Kevin Xu
Matt Blaze
University of Pennsylvania

HOW TO IMPROVE

Users lack intuition about complex computing devices →

Provide security education and training

Users are in charge of their own (complex) devices →

Make security invisible

It is hard to estimate risks →

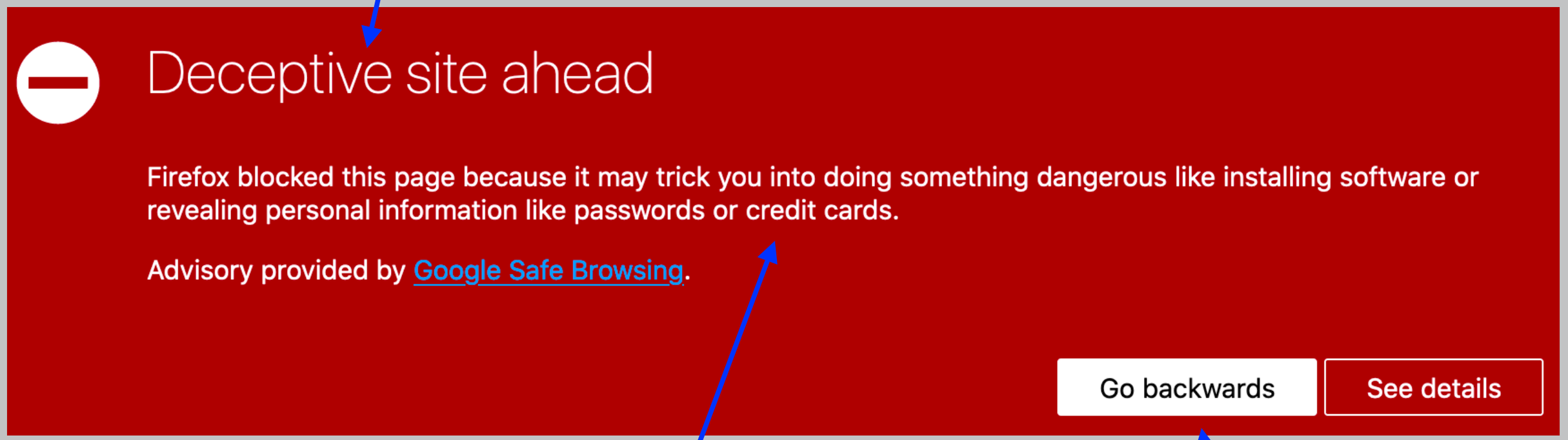
Help users build more accurate mental models

Security measures feel like they get in the way →

Make security the path of least resistance

SECURITY WARNINGS

warning is **brief**

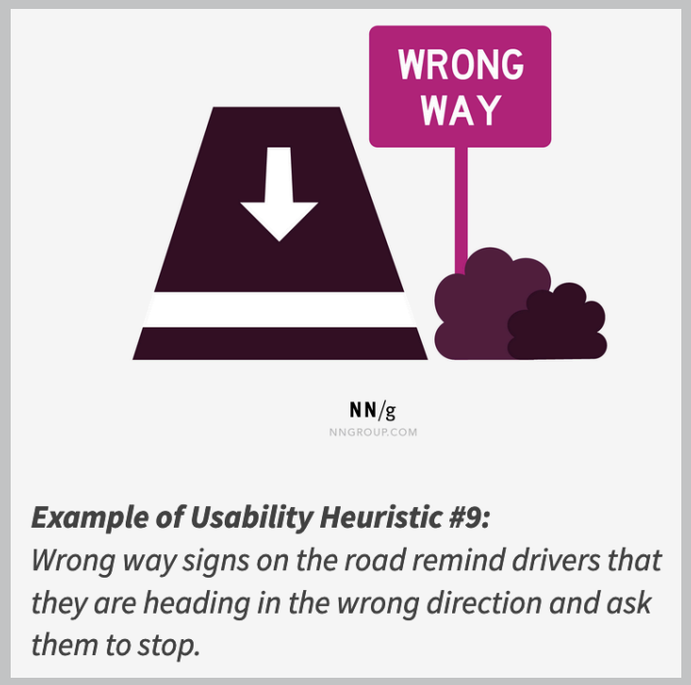


uses **simple language** to describe a **specific risk**

visual design makes the secure option look more **attractive**

USABILITY HEURISTICS

Great example of Neilsen's 9th usability heuristic: "Help users recognise, diagnose, and recover from errors"



Example of Usability Heuristic #9:
Wrong way signs on the road remind drivers that they are heading in the wrong direction and ask them to stop.

Other ones include:

- Recognition rather than recall (reduce memory burden)
- Design that speaks the user's language (mental models)
- Visibility of system status (feedback)

MAKING SECURITY EASIER

Need to:

- Minimise effort (workload and complexity)
- Support and guide users through design

Security **habits** must become “unconscious competence”

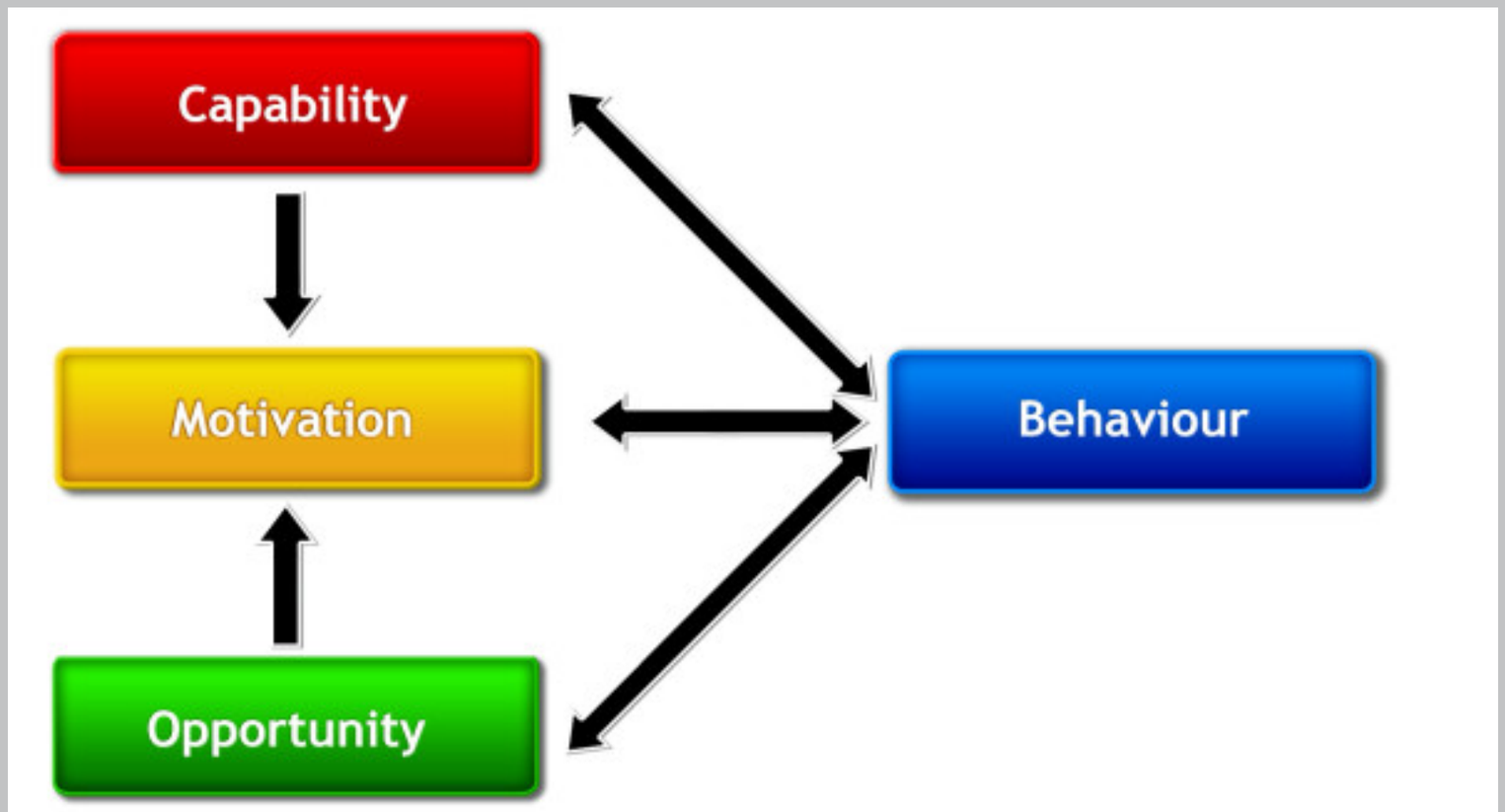
But how do we actually change these habits?

COM-B SYSTEM

ARE THEY ABLE TO?

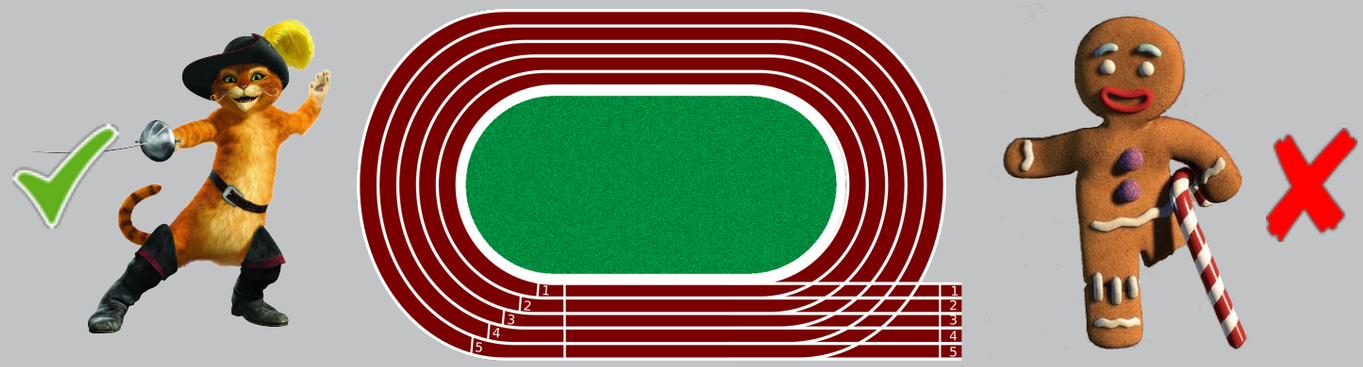
DO THEY WANT TO?

CAN THEY?



generalises for many different user groups
(just different obstacles for different groups)

IS THE SYSTEM USABLE?



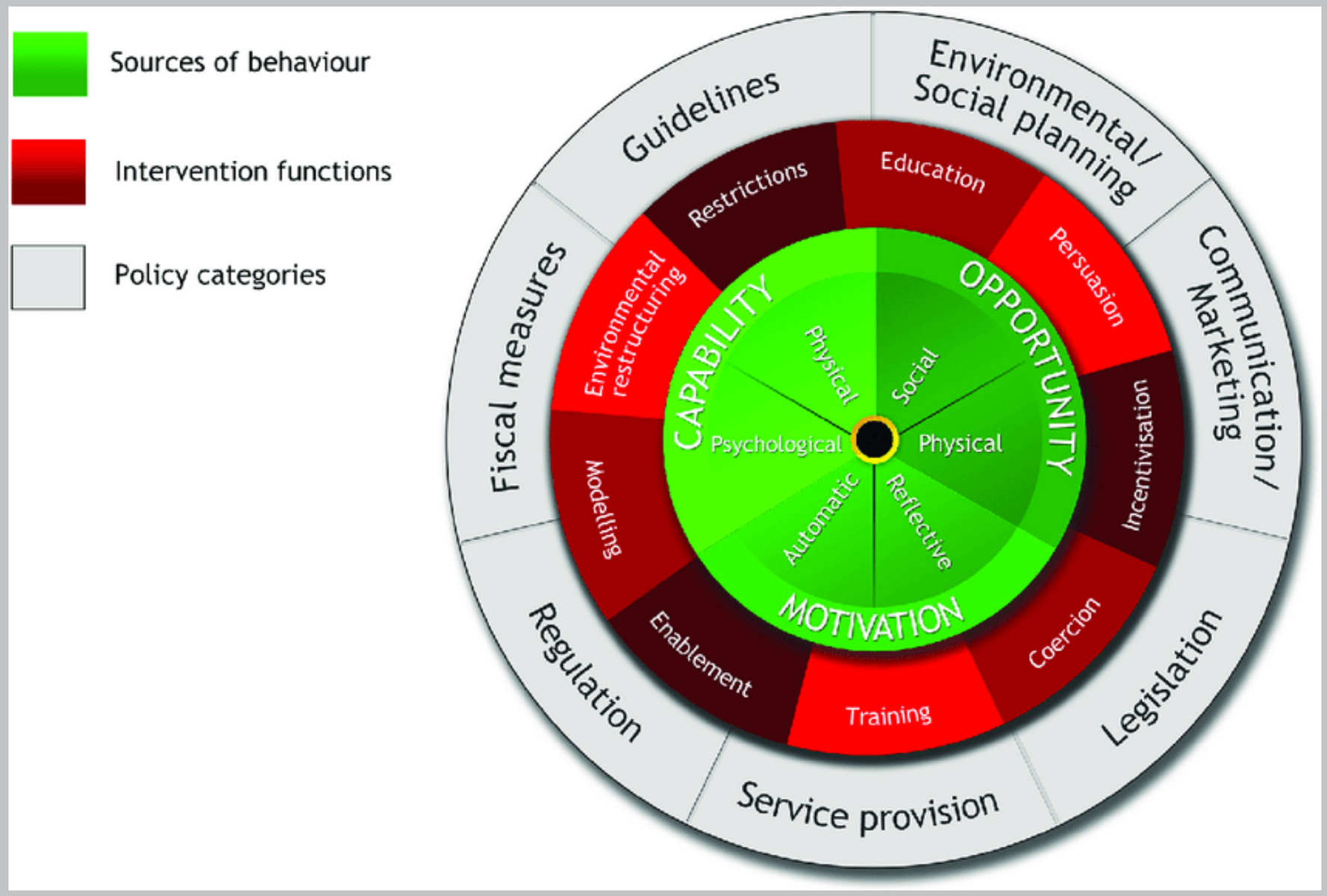
Need to instead ask: Is it usable for this user with this goal?

Not all users are the same: employees at a university, older adults, children, women, blind people, refugees, journalists, etc.

Even the same user can act differently (busy, on their laptop, etc.)

Not all goals are the same: employees use company devices for work, members of the public use mobile devices for social media, communication, gaming, navigation, etc.

COM-B SYSTEM



see a range of different approaches that can influence behaviour
(useful for far more than just computer security!)

HOW TO IMPROVE

Users lack intuition about complex computing devices →

Provide security education and training

Users are in charge of their own (complex) devices →

Make security invisible

It is hard to estimate risks →

Help users build more accurate mental models

Security measures feel like they get in the way →

Make security the path of least resistance

QUIZ!

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2821872`

to take this week's quiz!