Cabinet Office

Jenny Duckett
Senior Developer
Government Digital Service
@jenny_duckett

I'm from the UK Government Digital Service (GDS)

GOV.UK

Welcome to GOV.UK

The best place to find government services and information
Simpler, clearer, faster

Search GOV.UK

Popular on GOV.UK

- Universal Jobmatch job search
- Renew vehicle tax
- Log in to student finance
- Book your theory test
- Personal tax account

Benefits
Includes tax credits, eligibility and appeals

Births, deaths, marriages and care
Parenting, civil partnerships, divorce and Lasting Power of Attorney

Business and self-employed
Tools and guidance for businesses

Childcare and parenting
Includes giving birth, fostering, adopting, benefits for children, childcare and schools

Citizenship and living in the UK
Voting, community participation, life in the UK, international projects

Crime, justice and the law
Legal processes, courts and the police

Disabled people
Includes carers, your rights, benefits and the Equality Act

Driving and transport
Includes vehicle tax, MOT and driving licences

Education and learning
Includes student loans, admissions and apprenticeships

Employing people
Includes pay, contracts and hiring

Environment and countryside
Includes flooding, recycling and wildlife

Housing and local services
Owning or renting and council services

Money and tax
Includes debt and Self Assessment

Passports, travel and living abroad
Includes renewing passports and travel advice by country

Visas and immigration
Visas, asylum and sponsorship

Working, jobs and pensions
Includes holidays and finding a job

First, a sad story

Alice Bartlett @alicebartlett · May 13

Replying to @alicebartlett

The one I've done before was OK but all the examples were sexist so F[illegible] THAT

1 1 4

Alice Bartlett @alicebartlett · May 13

eg literally every person in a scenario who introduced a loophole was a woman, and everyone who fixed it was a man.

1

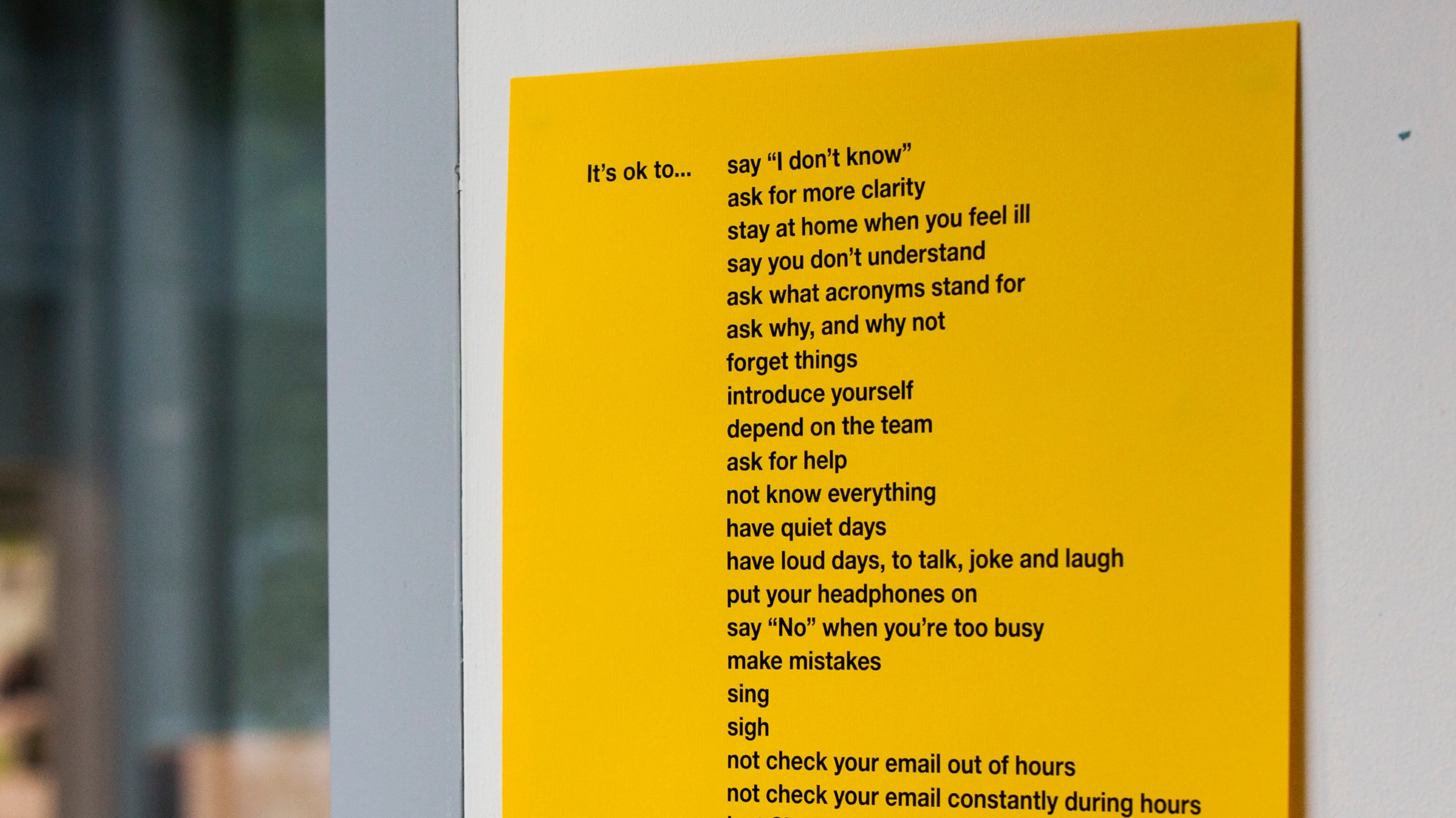
Alice Bartlett @alicebartlett · May 13

The trainer kept using phrases like "silly girl has done X"

6 1

Inappropriate content :-(

Why run a workshop?


It's ok to...
say "I don't know"
ask for more clarity
stay at home when you feel ill
say you don't understand
ask what acronyms stand for
ask why, and why not
forget things
introduce yourself
depend on the team
ask for help
not know everything
have quiet days
have loud days, to talk, joke and laugh
put your headphones on
say "No" when you're too busy
make mistakes
sing
sigh
not check your email out of hours
not check your email constantly during hours

Show that it’s ok to take time out to learn

Scale your impact

We’re all responsible for what we build

Why focus on security?

Developers often don’t feel confident about security

Expand the community of interested people

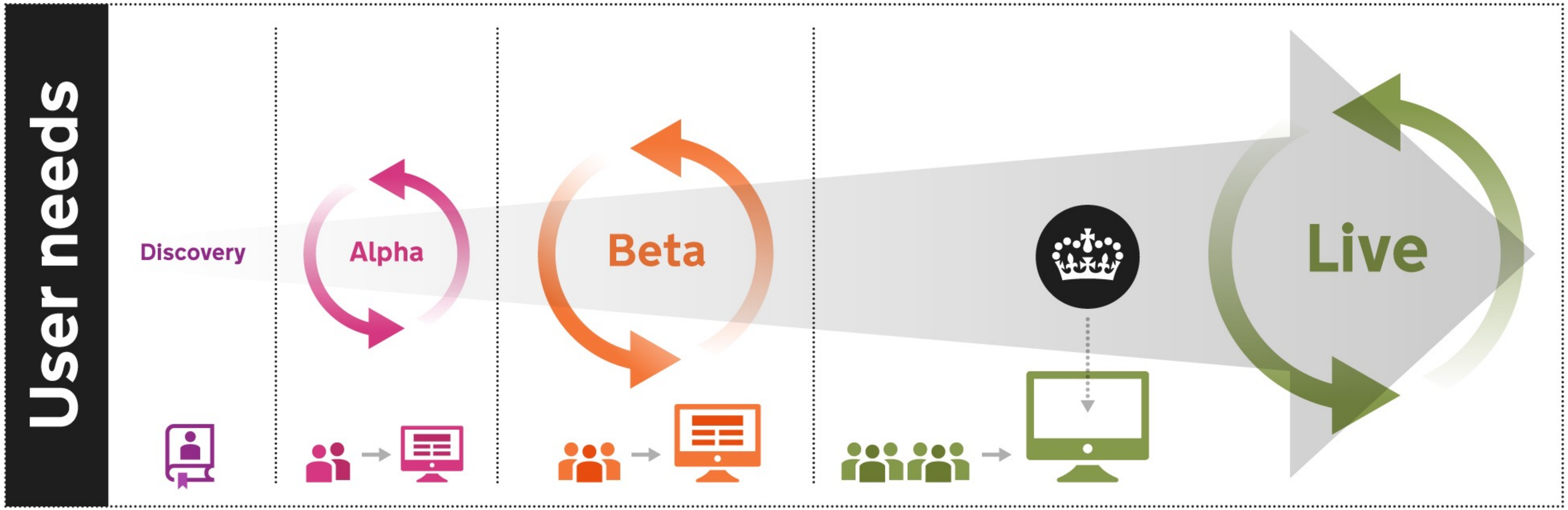
Security is one of many areas we care about

But I’m not a security expert!

…so I can’t do this

…~~so I can’t do this~~

…that’s fine, do it anyway


User needs
Discovery
Alpha
Beta
Live

Treat it as an alpha - prototype and iterate

You don’t have to cover everything

Experts aren’t always the best teachers

It isn’t about having all the answers

Find someone to work with

Alex Muller
(with egg for scale)

Hypotheses to test

The OWASP top 10 is a good starting point

OWASP Top 10 – 2013 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

Keep a strong practical focus

Make it a single day

Use the source code of exercises to learn

Government Digital Service

Aviation House, 125 Kingsway, Holborn, L... https://gds.blog.gov.uk/

Repositories | People 44

Search repositories... | Type: All | Language: All

whitehall

Publishes government content on GOV.UK

govuk | govuk-publishing-frontend

Ruby ★ 399 156 Updated 18 seconds ago

smart-answers

Serves smart answers on GOV.UK

govuk | govuk-publishing-frontend

Ruby ★ 90 85 Updated 19 seconds ago

digitalmarketplace-buyer-frontend

Frontend buyer application for the digital marketplace

digitalmarketplace

Python 5 Updated a minute ago

paas-rds-broker

Top languages

Ruby Python JavaScript CSS Go

Most used topics

govuk | govuk-publishing-frontend | verify | digitalmarketplace | govuk-pay

People 44 >

Learn how to use your everyday tools better

OWASP / railsgoat

A vulnerable version of Rails that follows the OWASP Top 10 http://railsgoat.cktricky.com

1,055 commits **6** branches **0** releases **20** contributors MIT

Branch: **master** New pull request Create new file Upload files Find file Clone or download

cktricky committed on **GitHub** Merge pull request #253 from jasnow/master ... Latest commit 3474385 on Dec 17, 2016

app	removed comments and Fixed Issue #184	a year ago
config	Fix METHOD for forgot_password route	a year ago
db	Upgraded simplecov and poltergeist gems	a year ago
doc	made some changes to the application controller, added a user control...	4 years ago
gauntlt_scripts	adding simple sqlmap gauntlt script, WIP	4 years ago
lib	Based on cane gem, removed tab indents and trailing blanks	2 years ago
log	made some changes to the application controller, added a user control...	4 years ago
public	More Rails 4.0 upgrade changes	3 years ago
script	adding vagrant and docker files	3 years ago
spec	Fixes #165	a year ago

Bring it home by using examples from your own applications

Get people to work together and help each other

Make something that other people can build on

Practical tips

About 15 people, with a range of skills

Ask people to set up in advance

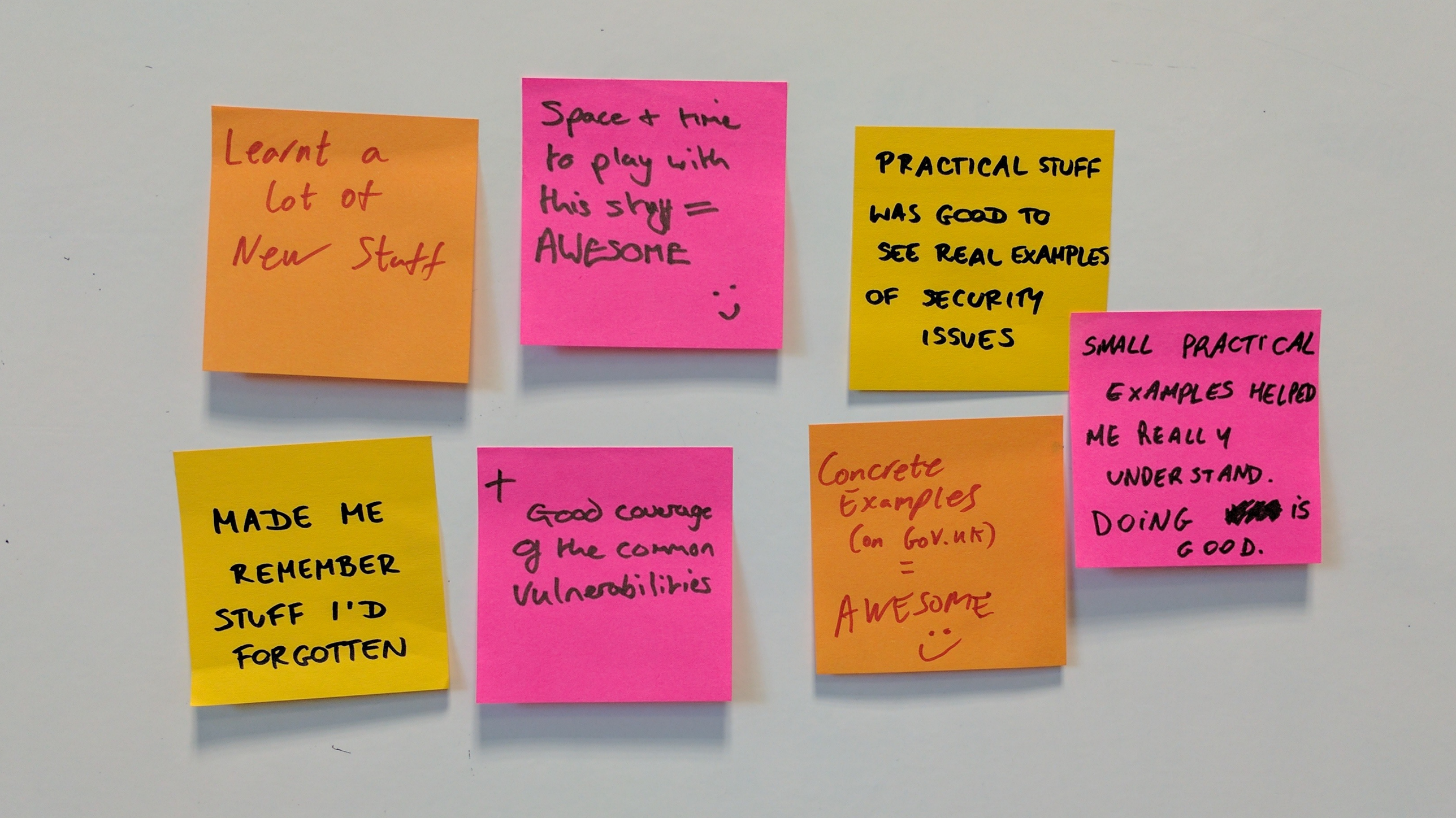
Set up a local network

Run a short retrospective

Ask for volunteers to run the next one

What did we learn?

It’s totally possible to do this!


Learnt a lot of New Stuff
Space + time to play with this stuff = AWESOME :)
PRACTICAL STUFF WAS GOOD TO SEE REAL EXAMPLES OF SECURITY ISSUES
SMALL PRACTICAL EXAMPLES HELPED ME REALLY UNDERSTAND. DOING [redacted] IS GOOD.
MADE ME REMEMBER STUFF I'D FORGOTTEN
+ Good coverage of the common Vulnerabilities
Concrete Examples (on GOV.UK) = AWESOME :)

You'll learn about the topic in more depth by preparing to explain it

Be ruthless with your MVP

Running the day well takes effort

Organising an event can be time-consuming

- organising space, facilities and people
- researching topics
- structuring the content
- writing presentations
- preparing practical exercises

What happened next?

Share what you’ve made

Blog

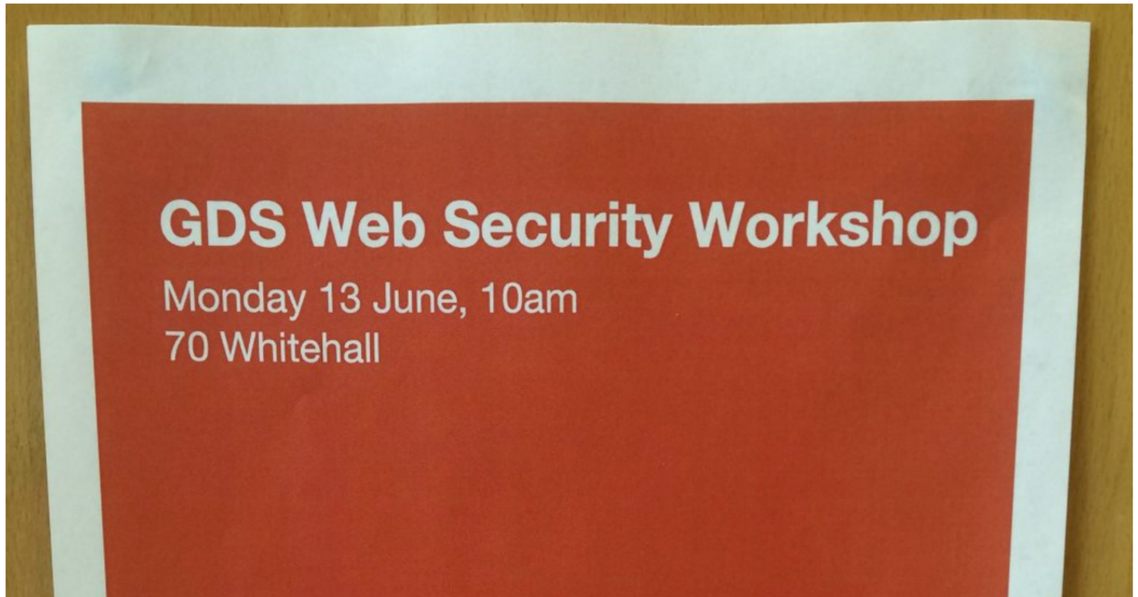
Technology at GDS

Search blog

Organisations: Government Digital Service

Our web security workshop for GDS developers

Alex Muller and Jenny Duckett, 9 August 2016 — Chat



GDS technology

A blog about how GDS builds, assembles and runs its software. Find out more.

Categories

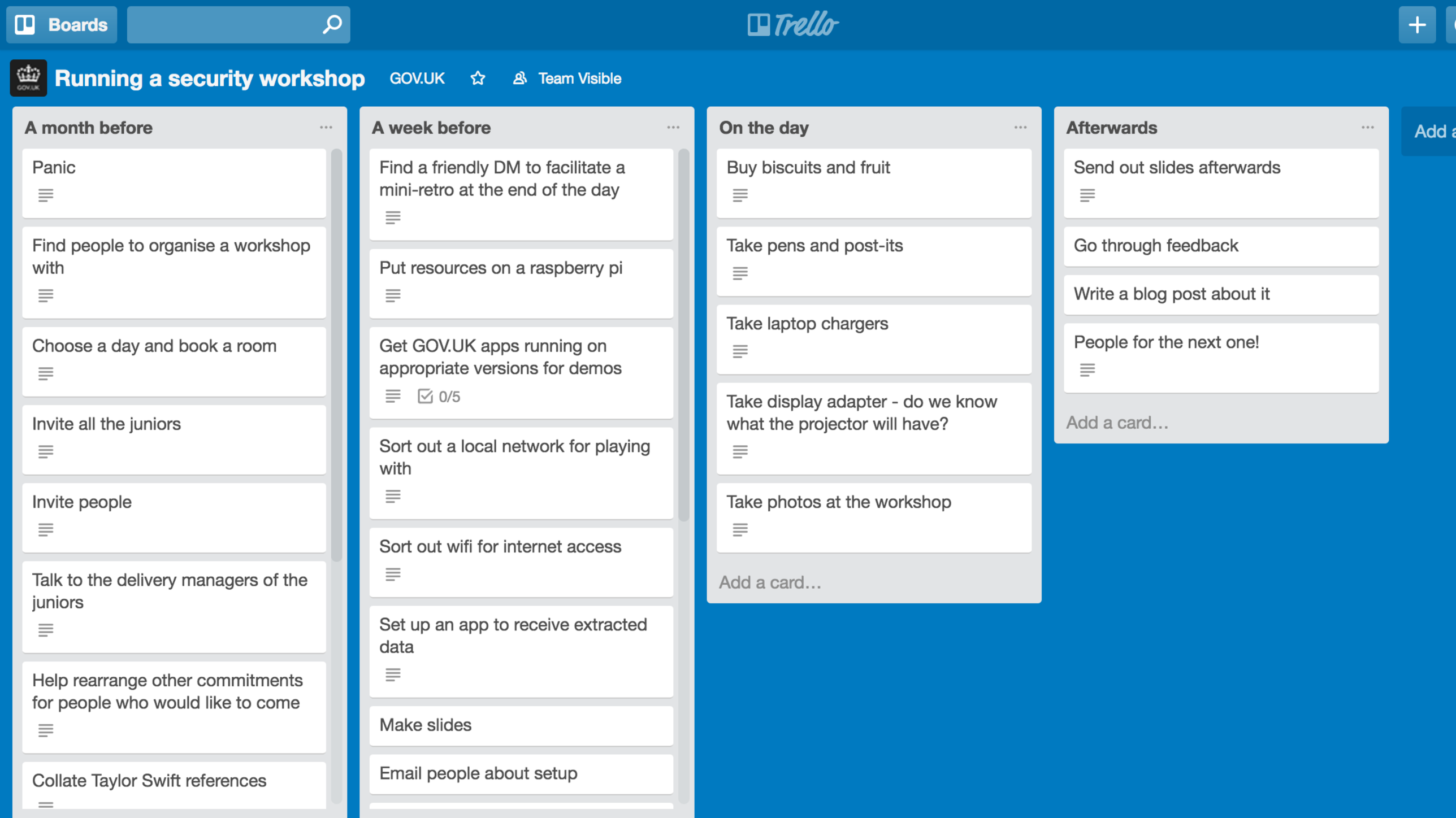
Select Category

Sign up for updates

Email Atom

Find out more

Join the conversation


Boards
Trello
Running a security workshop
GOV.UK
Team Visible
A month before
Panic
Find people to organise a workshop with
Choose a day and book a room
Invite all the juniors
Invite people
Talk to the delivery managers of the juniors
Help rearrange other commitments for people who would like to come
Collate Taylor Swift references
A week before
Find a friendly DM to facilitate a mini-retro at the end of the day
Put resources on a raspberry pi
Get GOV.UK apps running on appropriate versions for demos
0/5
Sort out a local network for playing with
Sort out wifi for internet access
Set up an app to receive extracted data
Make slides
Email people about setup
On the day
Buy biscuits and fruit
Take pens and post-its
Take laptop chargers
Take display adapter - do we know what the projector will have?
Take photos at the workshop
Add a card…
Afterwards
Send out slides afterwards
Go through feedback
Write a blog post about it
People for the next one!
Add a card…
Add a

Fix the biggest problem for next time

Support the people who come after you

2 workshops have happened since ours

They’ve taken the format forward in exciting ways we didn’t expect


Exit
PUSH
PUSH
Google

Workshops aren’t the end of the journey

You can do this too

What can you run a workshop about?

Jenny Duckett

@jenny_duckett

You don't need to be an expert on a topic to help people understand it - creating an opportunity to learn more about it together works too

RETWEETS	LIKES
3	9

You can encourage a culture of learning in your organisation

Cabinet Office

Thanks!

@jenny_duckett