Cyber Defence
@IETF

UK National Cyber Security Centre

NCSC does Active Cyber Defence

We protect UK users from ~~winged ninja cyber monkeys~~
high volume, low sophistication criminal attacks

- Phishing take-down
- Spoof e-mail detection with DMARC
- Malware detection in public sector DNS
- Find weak TLS and invalid X.509 certs on .gov.uk web servers
- Tackle the BGP hijack problem
- Gather data on security of UK SS7 terminations

Takedown of phishing websites

In 2017 we removed:
18,067 unique websites pretending to be a UK government brand

121,479 total unique phishing websites hosted in the UK

Reduced UK-hosted share of global phishing hosting from 5.5% to 2.9%

79,567 attacks prevented

Phishing has reduced **from 45 hours to 7 hours** from infringing of the government brand.

The average time a phishing site is online has reduced **from 27 hours to just 1 hour.**

DMARC

- Aim to stop delivery of e-mail with spoofed .gov.uk “From” address
- Driving adoption of DMARC / SPF for .gov.uk domains
- Increased support for DMARC from 5.6% to 18.3%
- Millions of spoofed e-mails being detected/stopped – thanks, DMARC!

What about the winged ninja cyber monkeys?

- NCSC has dealt with 1000+ nationally significant cyber attacks in 18 months
- We’ll be pulling out the root causes and publishing the data

- Socio-technical research
  - End-user training for anti-phishing isn’t enough
  - Realistic password policies

What we want to do

Produce, share and promote evidence-based research on:

- the effects of protocol design on cyber defence
- cyber attacks and how to detect and defend against them
- which counter-measures work, and which don’t

… and do this systematically across the IETF …

… and encourage others across industry to do the same …

… so that protocol designers can make better informed decisions.

How do we do this?

- An IRTF research group?
- A workshop (like ANRW?)
- SecDir review process

Who will help?

Come talk to us!