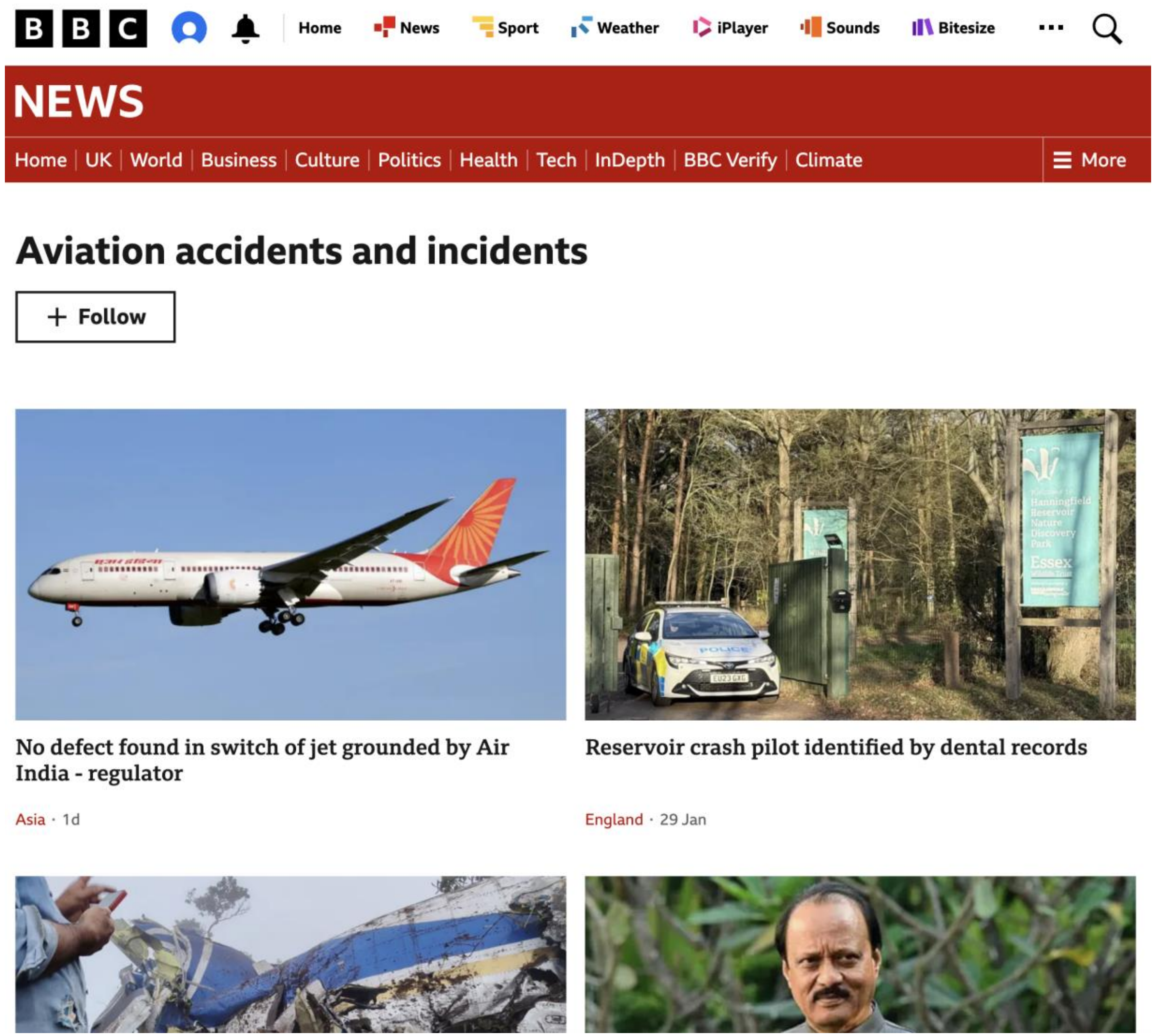
Security Engineering Feed Forward Session

5/2/2026

What is a threat assessment

- Not about recommending Controls
- Evidence based
- Balancing global and local information
- Identifying what to pay attention to (and also what not to!!!)
- Be **specific** about capabilities and likely tactics employed by threat actors

Evidence based


BBC
Home
News
Sport
Weather
iPlayer
Sounds
Bitesize
NEWS
Home | UK | World | Business | Culture | Politics | Health | Tech | InDepth | BBC Verify | Climate
More
+ Follow

Aviation accidents and incidents

No defect found in switch of jet grounded by Air India - regulator

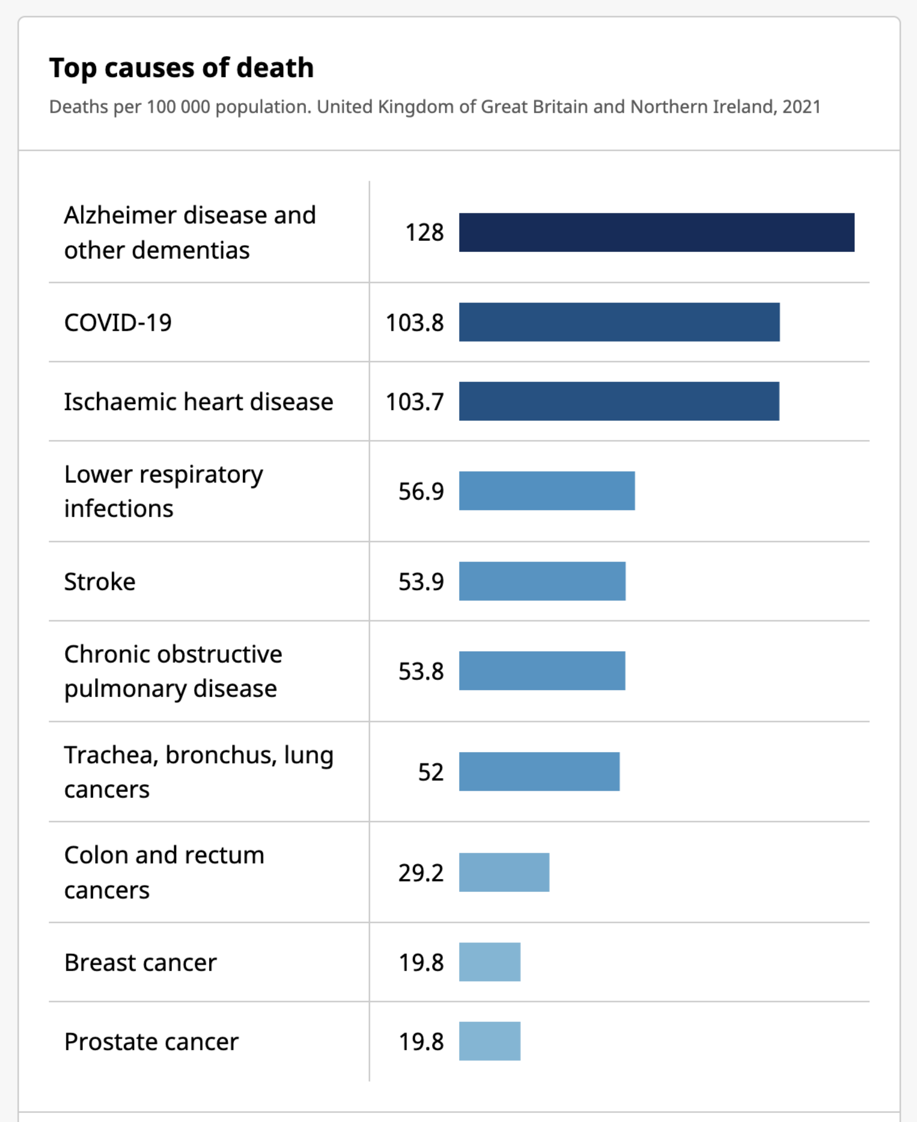
Asia · 1d

Reservoir crash pilot identified by dental records

England · 29 Jan

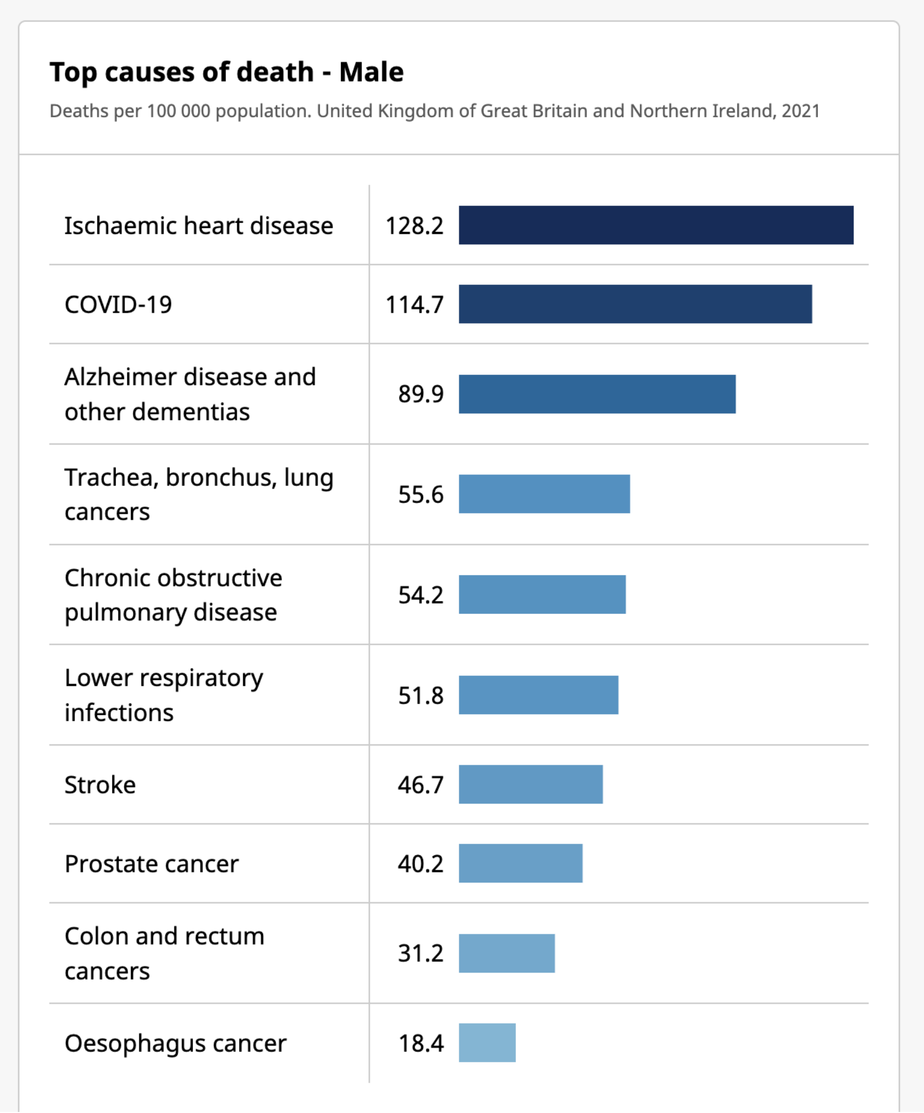
The 2023 death rate for air passengers was 0.003 deaths per 100 million miles. The rate for car and truck passengers was 0.53

Balancing global vs local information



Top causes of death

Deaths per 100 000 population. United Kingdom of Great Britain and Northern Ireland, 2021

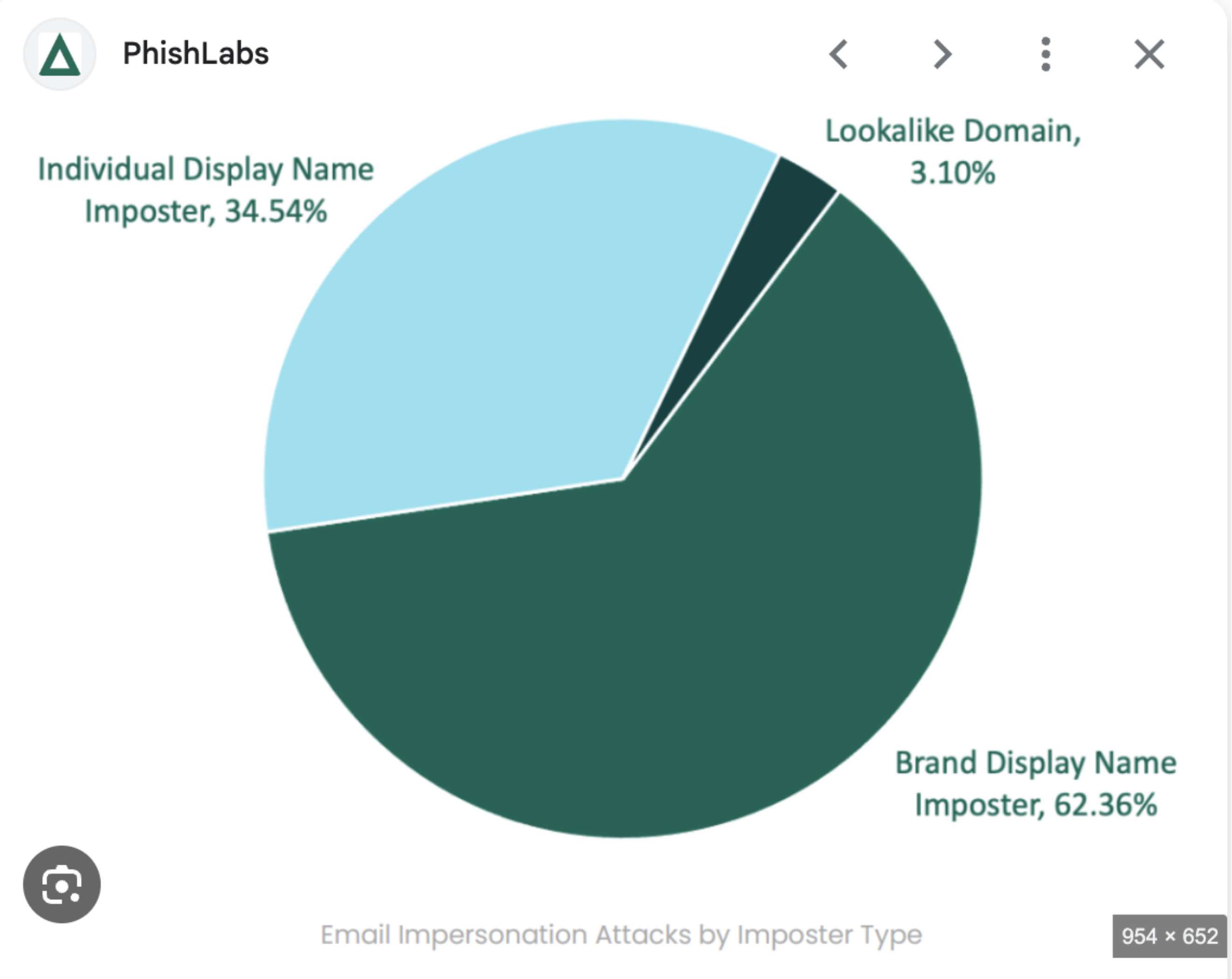


Top causes of death - Male

Deaths per 100 000 population. United Kingdom of Great Britain and Northern Ireland, 2021

Specificity

Phishing vs


PhishLabs
Individual Display Name Imposter, 34.54%
Lookalike Domain, 3.10%
Brand Display Name Imposter, 62.36%
954 × 652

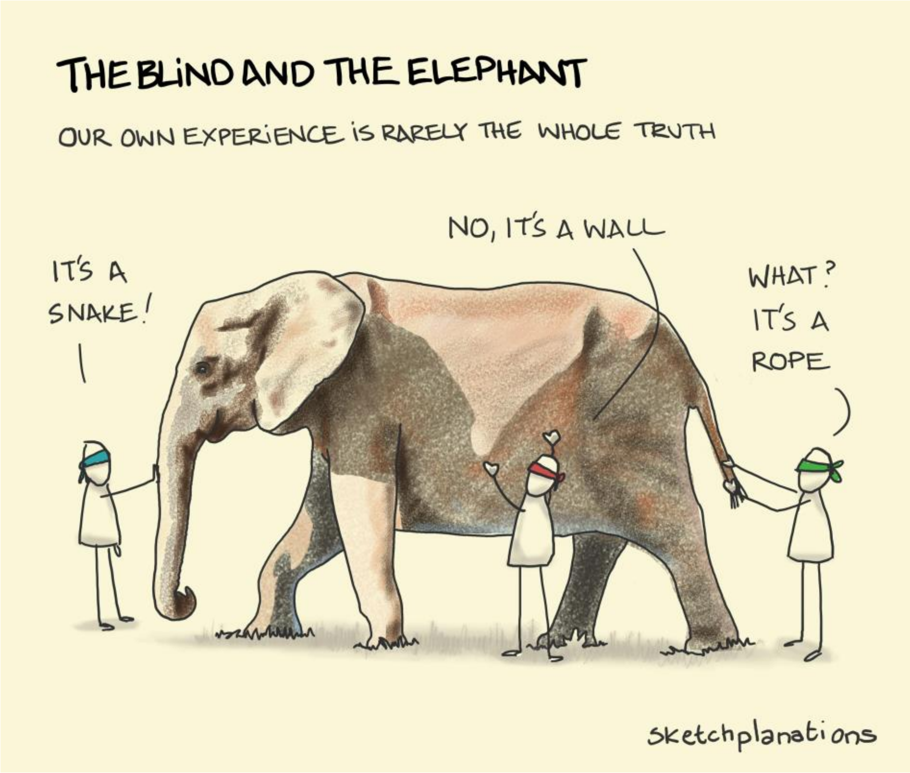
Email Impersonation Attacks by Imposter Type

Prioritization

- Based on what?
    - Likelihood vs impact vs risk
    - What can't be measured
        - Impact that can't be quantified
        - Incidents that aren't reported

Think critically

- Every source has limitations
  - Triangulation helps to cancel out biases


THE BLIND AND THE ELEPHANT
OUR OWN EXPERIENCE IS RARELY THE WHOLE TRUTH
IT'S A SNAKE!
NO, IT'S A WALL
WHAT? IT'S A ROPE
sketchplanations

In groups of 2-4, discuss the following:

What are the strengths and limitations of the following data sources for threat assessment:

- Vendor reports about attacks against their customers
- Law enforcement data about the frequency and impact of crimes
- Insurance data about the frequency and impact of claims
- News reports about how children are impacted by new tech

Strengths and Limitations

- Vendor reports about attacks against their customers
  - Know how it happened, but selection bias.. Unlikely to see all attackers, e.g. your email provider doesn't hear about malware infection
- Law enforcement data about the frequency and impact of crimes
  - Not all victims report, not all incidents are crimes, may not know how to quantify all harms (e.g. emotional, business outage etc).. Likely just money stolen
- Insurance data about the frequency and impact of claims
  - Not all incidents are covered, bias in who is insured, not all impacts are quantified
- News reports about how children are impacted by new tech
  - Other sources have a reporting delay but this doesn't.. Problem is you don't know how prevalent it is

In groups of 2-4, identify:

- The most common type of phishing
- The most common source of DDoS
- The most common way ransomware gangs get in
- The most common type of social engineering

Try to get as granular as possible