# Differential Language of Cybersecurity Across the Lifespan

## 1. Core Idea

- People understand and talk about **cybersecurity differently** depending on their **age/life stage**.
- These differences shape **attitudes, behaviours, and vulnerabilities**.
- Goal: Improve design of security systems, training, and communication by adapting to age-specific perspectives.

## 2. Method

- Surveyed **503 participants** across 3 groups:
  - Children (11–18, n=146).
  - Working-age adults (≈36 yrs avg, n=211).
  - Older adults (60+, n=146).
- Asked: "What comes to mind when you hear the word *cybersecurity*?"
- Analyzed responses with:
  - **Frequency analysis** → most common words.
  - **TF-IDF** → which terms were unique to each group.
  - **LIWC** → psychological/emotional categories of words.

## 3. Results

### Shared concepts (all groups)

- **Common words**: password, protection, internet, virus, hacking.
- Shows a **universal prototype** of cybersecurity: "keeping safe from hackers, viruses, and data loss."

### Children (11–18)

- **Focus**: *social risks*.
- Keywords: cyber-bullying, strangers, Snapchat, Instagram, friends.
- Emotions: more **positive**, less **anxiety** than adults.
- Behaviour: share more online, more vulnerable to phishing/grooming.

- ⚡ Insight: For kids, cybersecurity = **online safety + social threats**.

### Working-Age Adults

- **Focus**: *technical & criminal threats*.
- Keywords: authentication, encryption, VPN, penetration, terrorism, stealing.
- Stronger sense of **responsibility** (protecting work systems, data).
- Emotions: more **anxiety**, less "social/emotional" framing.
- ⚡ Insight: For adults, cybersecurity = **protecting systems and data in professional settings**.

### Older Adults

- **Focus**: *intrusion + nuisance*.
- Keywords: control, intrusion, malware, nuisance, possessions, society.
- Behaviour: less likely to use strong PINs or biometrics, sometimes more cautious with disclosure.
- Emotions: show more **cognitive processing** (cause/effect), moderate anxiety.
- ⚡ Insight: For older adults, cybersecurity = **loss of control, annoyance, scams**.

## 4. Psychological Analysis (LIWC)

- **Children**: more positive emotions, social words.
- **Adults**: more anxiety, technical/cognitive terms.
- **Older Adults**: more reflective, "cause-effect" framing, concern about intrusion.

## 5. Implications

- **Education & Training** → must be age-specific.
  - Children: focus on **social media safety** + cyberbullying.
  - Adults: focus on **workplace risks** + phishing/crime.
  - Older adults: focus on **scam awareness** + confidence building.
- **System Design (SBD link)**:
  - Interfaces and warnings should adapt to user group needs.
  - Example: Kids → relatable, simple visuals. Adults → technical details. Seniors → clear, non-technical language.
- **Lifespan approach**: must consider how **cybersecurity needs shift across life stages**.

# Takeaway

Cybersecurity isn't just technical — it's **socially and psychologically shaped**.

- Kids: **safety in social spaces**.
- Adults: **technical defence + workplace security**.
- Seniors: **avoid scams, maintain control, reduce nuisance**.

👉 For *Secure by Design*: we must **design systems and training with age in mind**, not one-size-fits-all.