LETS TALK CYBER

Email Spoofing:	Deceptive Links:	Social Engineering:	Credential Theft:	Spear Phishing:
Vishing and Smishing:	Phishing susceptibility:	Weak Password Practices:	Social Engineering:	Lack of Security Awareness:
Failure to Update Software:	Unauthorized Device Usage:	Insufficient Privacy Settings:	USB and Removable Media Risks:	Unsecured Wi-Fi Connections:
Over reliance on Default Settings:	Failure to Report Security Incidents:	Inadequate BYOD policies:.	Unrestricted Access Permissions:	Human Error:

The Human Factor of Cyber security – How are you communicating?

What is cyber security?

- Tools and practices to keep you safe online.
- (Platforms, Processes, People)
- The Internet is very resourceful. Internet connectivity enables a lot of aspects of our everyday lives. However, being online without precaution can do more harm than good.
- So how do we encourage people to get online, and hand hold them to be safe online without scaring them away? -

Human Scenarios -

Adults – Susceptibility to fake news, online fraud, physical access to their devices, manipulation, too much tech.

Workplace – locking PC, online meetings, privacy, personal / official information.

Average person – No access control. Updating your device. Links.

Leaders – what is at stake?

Children – Downloading games and clicking links,

Digital skilling – Information upgrading

Call to action - Communicating cyber

Empowerment Over Fear. Dos alongside the don'ts

Relatable language / clarity: You are talking to yourselves

Highlight Personal and Financial Impact – What is at stake? Why should I care?

Relentless awareness – There is no winning!! The struggle continues

Digital literacy – relentless and continuous

Organizational culture of cyber security – influence us to change

Parents and care takers - Talk to the children about online behavior, data protection, AI, links.