CoGrammar

Welcome to this session:
Task 21 Walkthrough

The session will start shortly...

Questions? Drop them in the chat.
We'll have dedicated moderators answering questions.

Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly. **(Fundamental British Values: Mutual Respect and Tolerance)**
- No question is daft or silly - **ask them!**
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: **Questions**

Cyber Security Session Housekeeping

- For all **non-academic questions**, please submit a query: ***www.hyperiondev.com/support***
- **Report a safeguarding incident: *www.hyperiondev.com/safeguardreporting***
- We would love your feedback on lectures: Feedback on Lectures
- If you are hearing impaired, please kindly use your computer's function through Google Chrome to enable captions.

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:

Ian Wyles
Designated Safeguarding Lead

Simone Botes

Nurhaan Snyman

Rafiq Manan

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

or email the Designated Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

CoGrammar HyperionDev

Stay Safe Series:

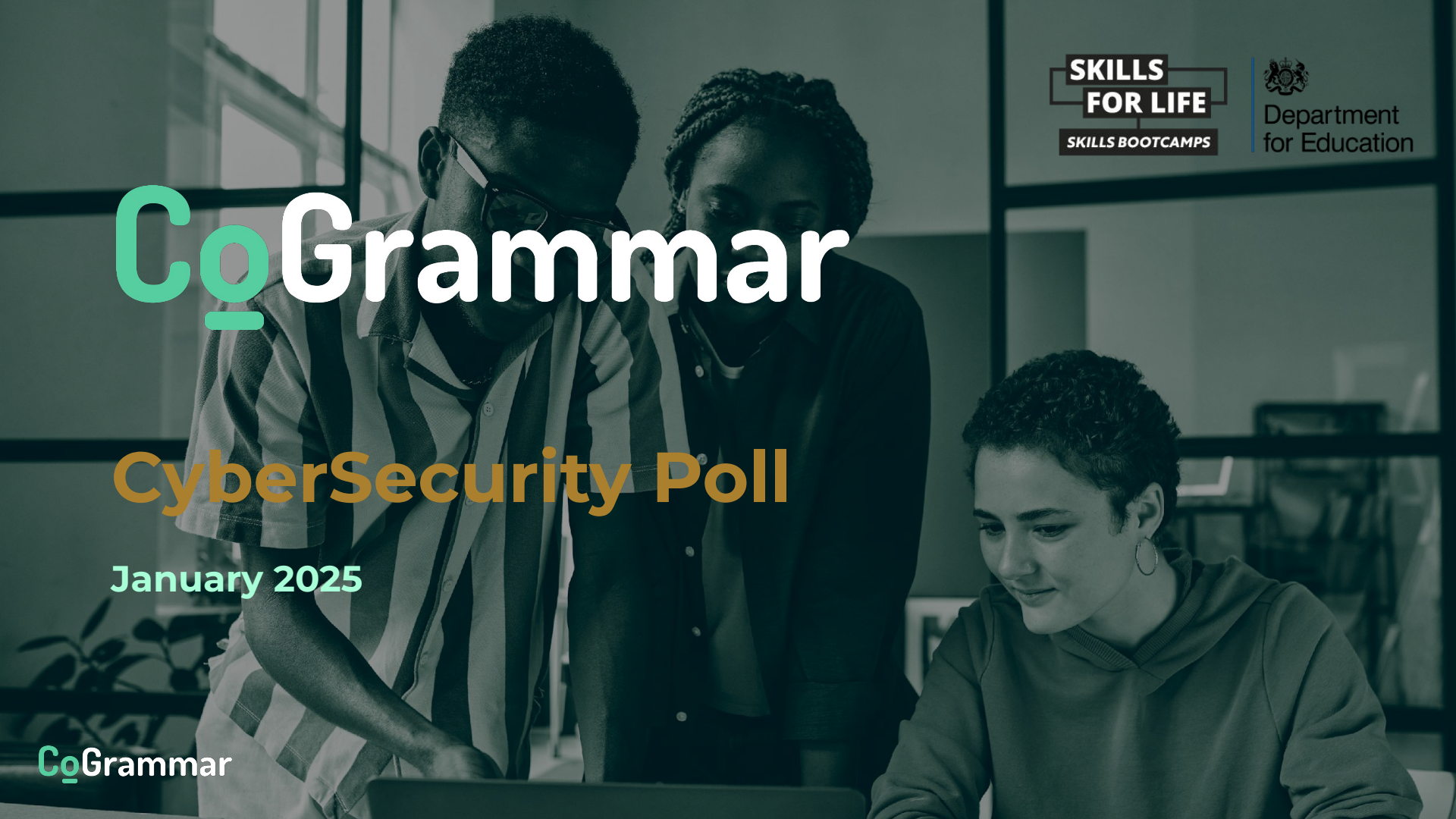
Mastering Online Safety One week at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalization, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the *Stay Safe Series* will guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.

Learning Objectives & Outcomes

- Define file-based input and dynamic evaluation in Python.
- Explain the risks associated with unsanitized inputs and the use of eval.
- Use alternative functions (e.g., int(), float()) to parse and handle inputs instead of eval.
- Develop a secure version of a file-processing script that resists common security exploits like code injection

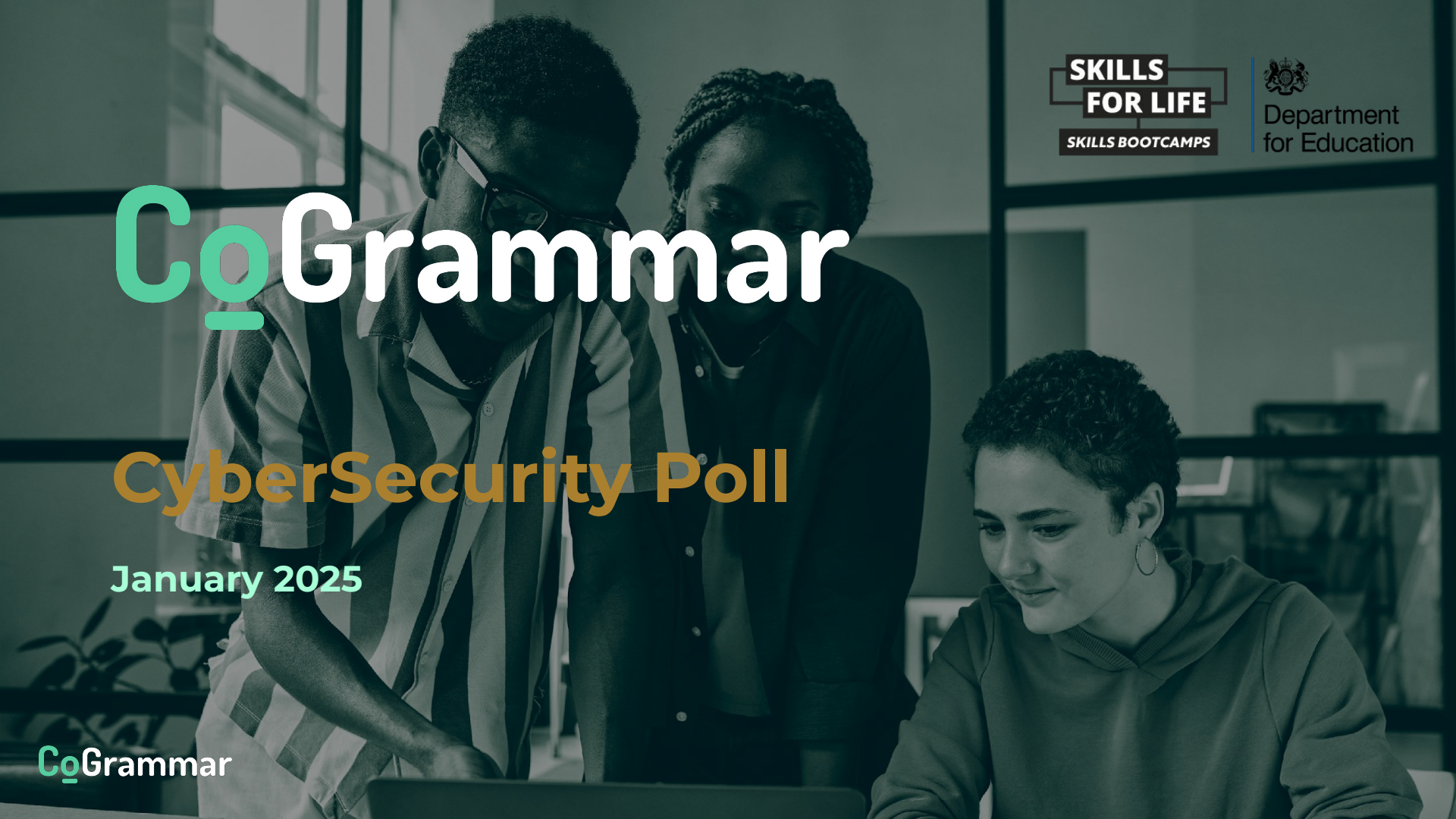

SKILLS FOR LIFE
SKILLS BOOTCAMPS
Department for Education
CoGrammar
CyberSecurity Poll
January 2025
CoGrammar

Key Terms

- **File-based input handling:** Programs often read data from files to perform actions.
- **Security risks with dynamic evaluation:** Functions like eval can execute malicious code if inputs are not properly sanitized.

Task at hand

- Call the hack() function using file based input for hack1.py, hack2.py and hack3.py


SKILLS FOR LIFE
SKILLS BOOTCAMPS
Department for Education
CoGrammar
CyberSecurity Poll
January 2025
CoGrammar

Questions and Answers

CoGrammar

Thank you for attending

CoGrammar

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education